Vnitřní LTE modem WF831

Uživatelská příručka

Rejstřík

1 Začínáme

1.1 Vítá vás nový LTE modem

V tomto dokumentu se nachází pojem CPE, který označuje LTE (Long Term Evolution) modem instalovaný jako customer-premises equipment, tedy přímo v domácnosti zákazníka. Seznamte se s významem následujících bezpečnostních symbolů, které vám pomohou s bezpečným a korektním použitím vašeho CPE:

	Přídavné informace
	Volitelné metody, případně zkratky určité akce
	Potenciální problémy nebo dále specifikovaná upozornění

1.2 Požadavky na hardwarovou výbavu počítače

Aby byl zaručen optimální výkon modemu, ujistěte se, že váš počítač splňuje následující minimální požadavky.

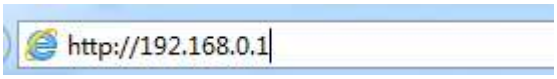
Položka	Požadavek
Procesor	Pentium 500 MHz nebo vyšší
Operační paměť	128 MB RAM nebo vyšší
Pevný disk	Alespoň 50 MB volného místa
Operační systém	• Microsoft: Windows XP, Windows Vista, Windows 7 a novější • Mac: Mac OS X 10.5 a novější
Rozlišení obrazovky	1024 × 768 pixelů nebo vyšší
Prohlížeč	• Internet Explorer 7.0 a novější • Firefox 3.6 a novější • Opera 10 a novější • Safari 5 a novější • Chrome 9 a novější

1.3 Přihlášení do webového rozhraní pro správu

Ke konfiguraci a správě vašeho CPE slouží webové rozhraní, do kterého se můžete přihlásit prostřednictvím webového prohlížeče.

Následující procedura popisuje způsob, jakým se na počítači s operačním systémem Windows XP a prohlížečem Internet Explorer 7.0 přihlásíte do webového rozhraní pro správu CPE.

1. Ujistěte se, že je jednotka CPE správně připojena.
2. Spusťte Internet Explorer, zadejte do adresního řádku http://192.168.0.1 a stiskněte klávesu Enter. Viz obrázek 1-1.



Obrázek 1-1

3. Zadejte uživatelské jméno a heslo a klepněte na tlačítko Login (přihlášení).

Po ověření zadaného hesla proběhne přihlášení do rozhraní pro správu. Viz obrázek 1-2.

Obrázek 1-2

Výchozí uživatelské jméno je **admin** a výchozí heslo **je stejné jako heslo k síti Wi-Fi**. Heslo k Wi-Fi síti najdete vytištěné na štítku zadní strany CPE.

Abyste vaše CPE ochránili před neautorizovaným přístupem, změňte výchozí heslo po prvním přihlášení.

CPE podporuje funkci diagnostiky. Pokud narazíte na problémy, obraťte se na středisko péče o zákazníky.

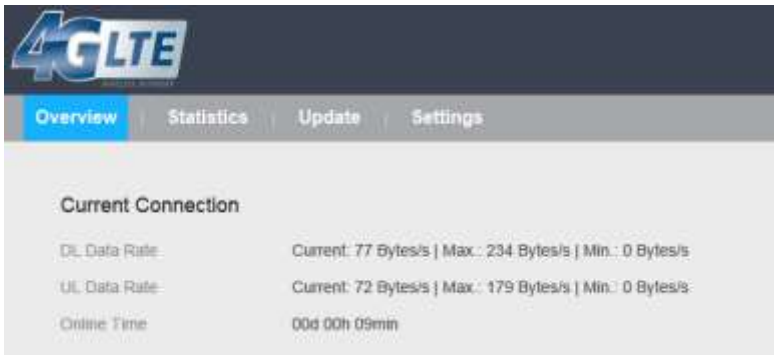
Aby byla zajištěna bezpečnost vašich dat, důrazně doporučujeme zapnout bránu firewall, a uchovávat veškeré přihlašovací údaje s maximální opatrností.

2 Přehled

2.1 Přehled o aktuálním připojení

Přehled o aktuálním připojení získáte následujícími kroky:

1. Klikněte na záložku **Overview** (Přehled).
2. V oblasti **Current Connection** (Stav připojení) budou zobrazeny podrobnosti o aktuálním stavu připojení, jako je rychlost stahování (download) a nahrávání (upload), a také čas připojení. Viz obrázek 2-1.

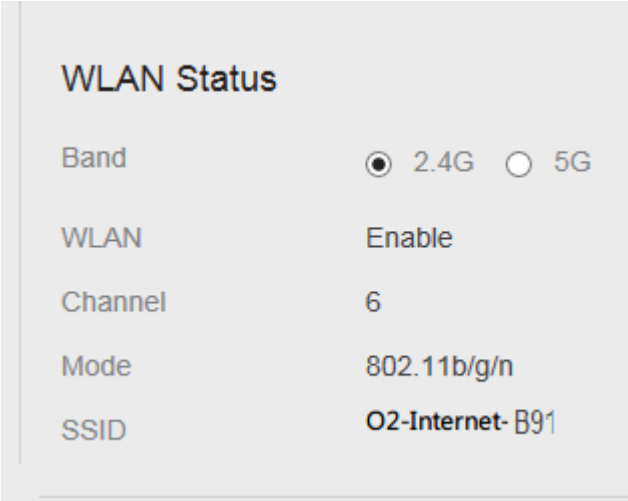


Obrázek 2-1

2.2 Přehled o stavu WLAN

Přehled o stavu WLAN získáte následujícími kroky:

1. Klikněte na záložku **Overview** (Přehled).
2. V oblasti **WLAN Status** (stav WLAN) budou zobrazeny informace o síti WLAN, jako je číslo kanálu, režim nebo SSID. Viz obrázek 2-2.

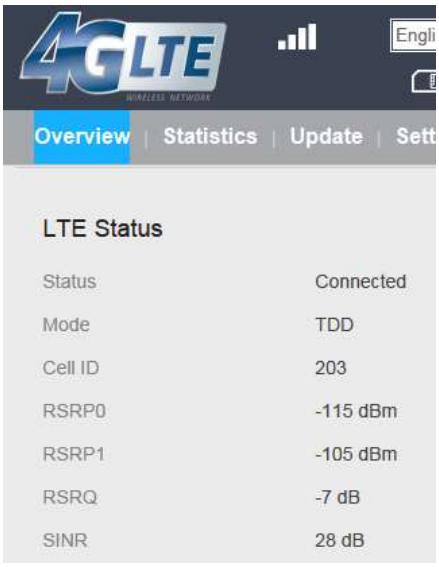


Obrázek 2-2

2.3 Přehled o stavu LTE

Přehled o stavu LTE získáte následujícími kroky:

1. Klikněte na záložku **Overview** (Přehled).
2. V oblasti **LTE Status** (stav LTE) budou zobrazeny informace o síti LTE, jako je režim, intenzita signálu nebo SINR. Viz obrázek 2-3.

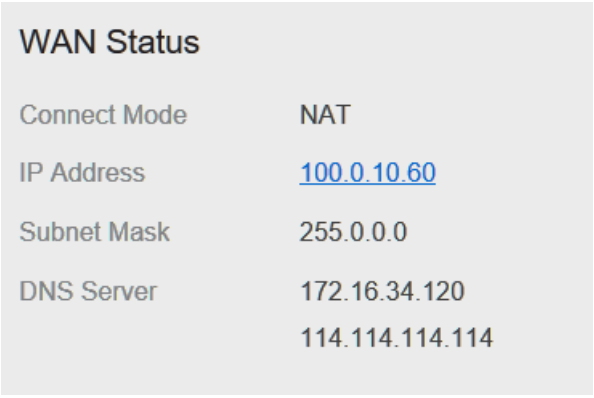


Obrázek 2-3

2.4Přehled o stavu WAN

Přehled o stavu WAN získáte následujícími kroky:

1. Klikněte na záložku **Overview** (Přehled).
2. V oblasti **WAN Status** (stav WAN) budou zobrazeny informace o režimu připojení, IP adresa, maska podsítě, server DNS a další. Viz obrázek 2-4.



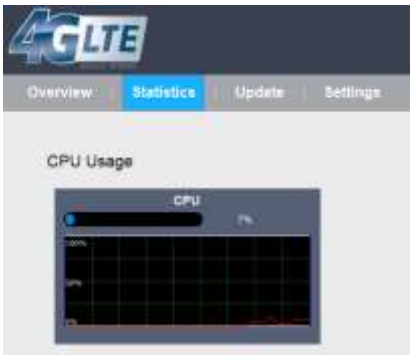
Obrázek 2-4

3 Statistiky

3.1 Vytížení procesoru

Přehled o vytížení procesoru získáte následujícími kroky:

1. Klikněte na záložku **Statistics** (Statistiky).
2. V oblasti **CPU Usage** (vytížení procesoru) bude zobrazena výkonová křivka vytížení procesoru. Viz obrázek 3-1.

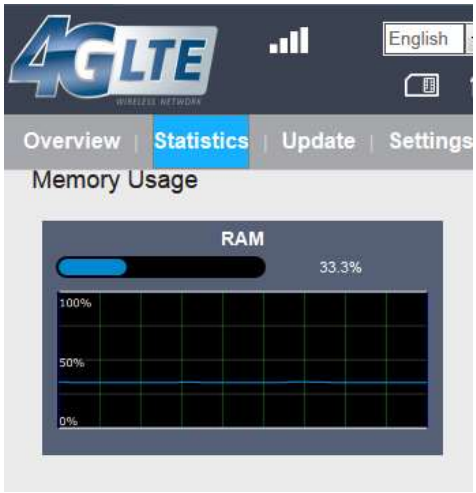


Obrázek 3-1

3.2 Vytížení operační paměti

Přehled o vytížení operační paměti získáte následujícími kroky:

1. Klikněte na záložku **Statistics** (Statistiky).
2. V oblasti **Memory Usage** (vytížení operační paměti) bude zobrazena výkonová křivka vytížení paměti. Viz obrázek 3-2.

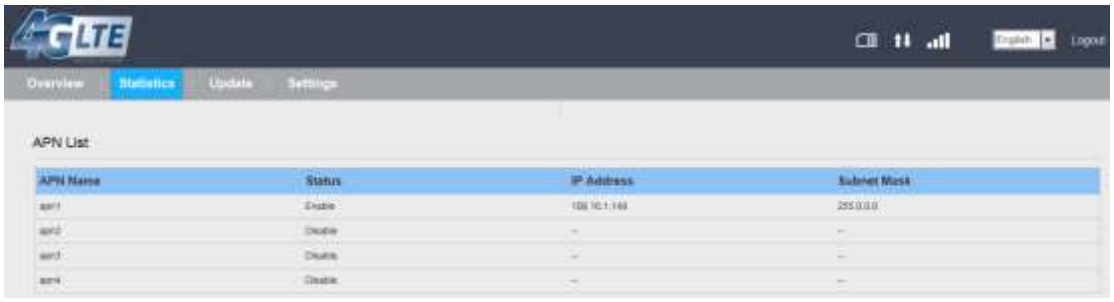


Obrázek 3-2

3.3 Zobrazení seznamu APN

Seznam dostupných APN získáte následujícími kroky:

1. Klikněte na záložku **Statistics** (Statistiky).
2. V oblasti APN List (seznam APN) budou zobrazeny dostupné APN, jejich stav a další informace. Viz obrázek 3-3.



Obrázek 3-3

3.4 Statistiky propustnosti

Přehled statistik propustnosti získáte následujícími kroky:

1. Klikněte na záložku **Statistics** (Statistiky).
2. V oblasti **Throughput Statistics** (statistiky propustnosti) budou uvedeny informace o propustnosti sítí WAN a LAN. Viz obrázek 3-4.

Obrázek 3-4

3.5 Zobrazení seznamu zařízení

Seznam připojených zařízení zobrazíte následujícími kroky:

1. Klikněte na záložku **Statistics** (Statistiky).
2. V oblasti **Device List** (Seznam zařízení) budou zobrazeny informace o zařízení připojených k vašemu CPE, např. název zařízení, adresy IP a MAC nebo doba zapůjčení přístupového tokenu. Viz obrázek 3-5.

Obrázek 3-5

4 Aktualizace

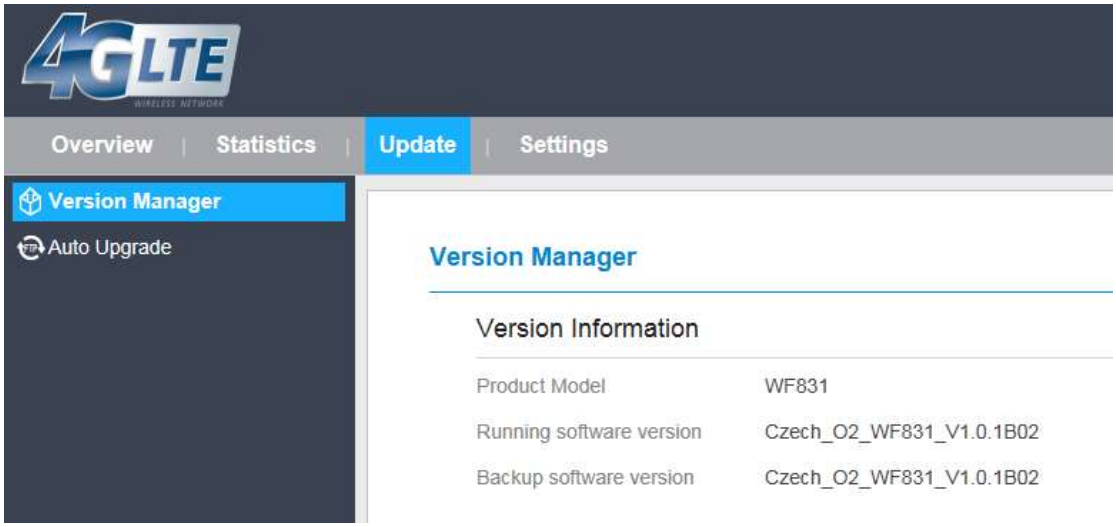
Prostřednictvím funkce aktualizace můžete aktualizovat software vašeho CPE na nejnovější verzi. Aktualizaci softwaru důrazně doporučujeme, protože nové verze přinášejí opravy chyb a všeobecné zvýšení stability systému.

4.1Správce verzí

4.1.1 Zobrazení aktuální verze

Aktuální verzi softwaru zařízení zobrazíte následujícími kroky:

1. Klikněte na volbu **Version Manager** (Správce verzí).
2. V oblasti **Version Info** (Informace o verzi) bude zobrazen název produktu a aktuální verze software. Viz obrázek 4-1.



Obrázek 4-1

4.1.2 Proces aktualizace

Pro úspěšné provedení aktualizace připojte CPE k počítači pomocí síťového kabelu a stáhněte do počítače soubor s aktualizací. Ujistěte se, že k CPE není připojeno nic jiného kromě napájecího adaptéru a počítače, na kterém se nachází aktualizační soubor.

Pro spuštění aktualizace proveďte následující kroky:

1. Klikněte na volbu **Version Manager** (Správce verzí).
2. V oblasti **Local Upgrade** (Aktualizace z místního souboru) klikněte na tlačítko **Browse** (Procházet). Zobrazí se dialogové okno prohlížeče souborů, jehož pomocí najděte soubor s aktualizací.

3. Klikněte na tlačítko **Open** (Otevřít). Dialogové okno se zavře. Cesta k souboru a jeho název budou nyní zobrazeny v poli Update file (Soubor s aktualizací).
4. Klepněte na **Aktualizovat**.
5. Aktualizace softwaru bude spuštěna. Po úspěšném dokončení aktualizace se CPE automaticky restartuje a bude spuštěna nová verze software. Viz obrázek 4-2.

⚠ V průběhu aktualizace CPE nevypínejte a neodpojujte od počítače.

Obrázek 4-2

5 Informace o zařízení

5.1 Zobrazení informací o systému

Informace o systému zobrazíte následujícími kroky:

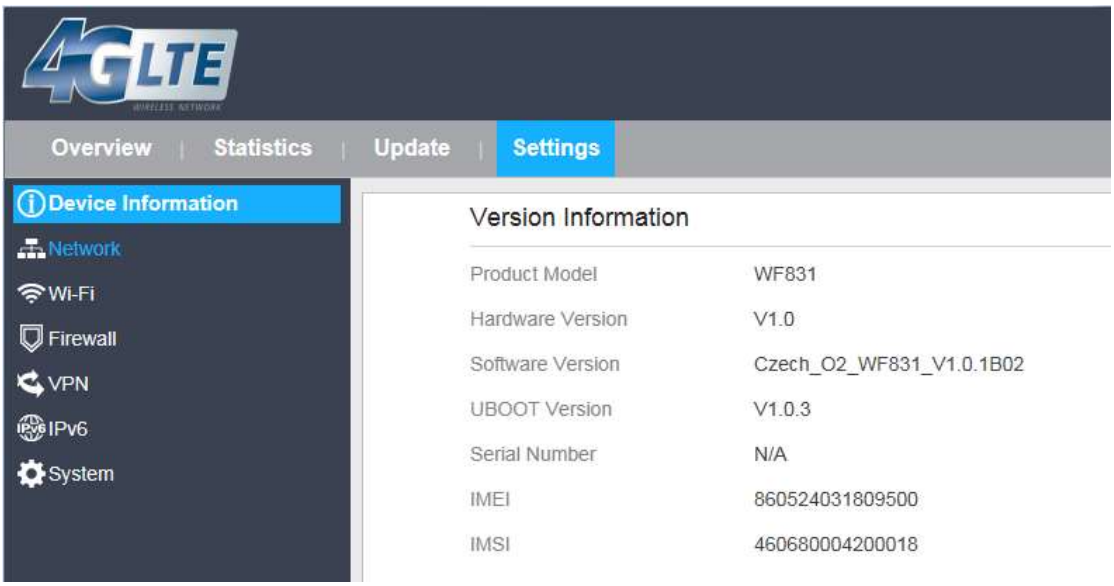
1. Přejděte do nabídky **Settings** (Nastavení) **> Device Information** (Informace o zařízení).
2. V oblasti **System Information** (Informace o systému) budou zobrazeny informace o stavu systému, např. provozní doba. Viz obrázek 5-1.

Obrázek 5-1

5.2 Zobrazení informace o verzi

Informace o verzi zobrazíte následujícími kroky:

1. Přejděte do nabídky **Settings** (Nastavení) **> Device Information** (Informace o zařízení).
2. V oblasti **Version Information** (Informace o verzi) budou zobrazeny informace o verzi zařízení a další podrobnosti, např. název produktu, verze software nebo verze zavaděče UBoot. Viz obrázek 5-2.



Obrázek 5-2

5.3 Zobrazení stavu LAN

Přehled o stavu LAN získáte následujícími kroky:

1. Přejděte do nabídky **Settings** (Nastavení) **> Device Information** (Informace o zařízení).
2. V oblasti **LAN Status** (Stav LAN) budou zobrazeny informace o připojení k síti LAN, např. adresy IP a MAC nebo maska podsítě. Viz obrázek 5-3.

Obrázek 5-3

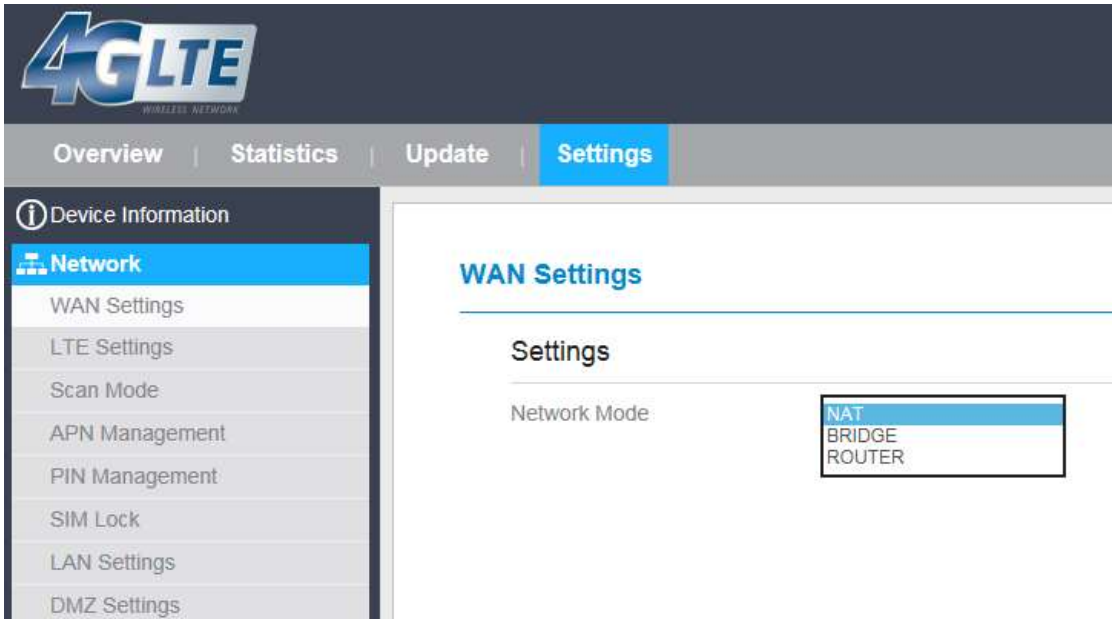
6 Nastavení sítě

6.1 Nastavení sítě WAN

6.1.1 Režim sítě

Nastavení režimu sítě je možné provést následujícími kroky:

1. Přejděte do položky **Settings** (Nastavení) **> Network** (Síť) **> WAN Settings** (Nastavení WAN).
2. V oblasti **Network Mode** (Režim sítě) vyberte jednu z možností **NAT**, **BRIDGE** nebo **ROUTER**.
3. Klikněte na tlačítko **Submit** (Uložit). Viz obrázek 6-1.



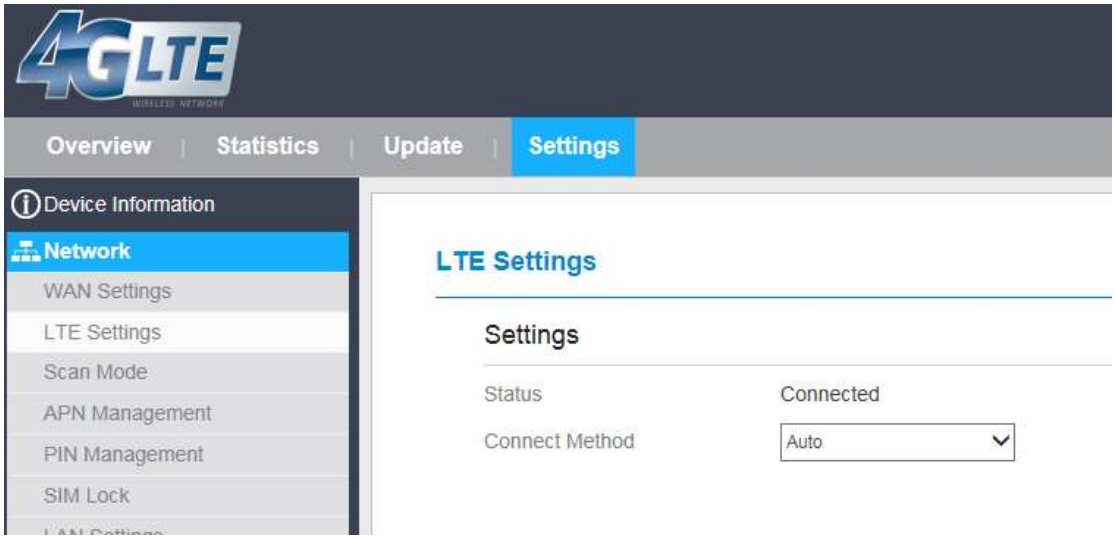
Obrázek 6-1

6.2Nastavení LTE

6.2.1 Nastavení LTE

Nastavení připojení LTE je možné provést následujícími kroky:

1. Přejděte do položky **Settings** (Nastavení) **> Network** (Síť) **> LTE Settings** (Nastavení LTE).
2. Oblast **LTE Settings** (Nastavení LTE) obecně obsahuje informace o stavu připojení k síti LTE, jako je frekvence, RSSI, RSRP, RSRQ, CINR, SINR, ID buňky a další. Viz obrázek 6-2.



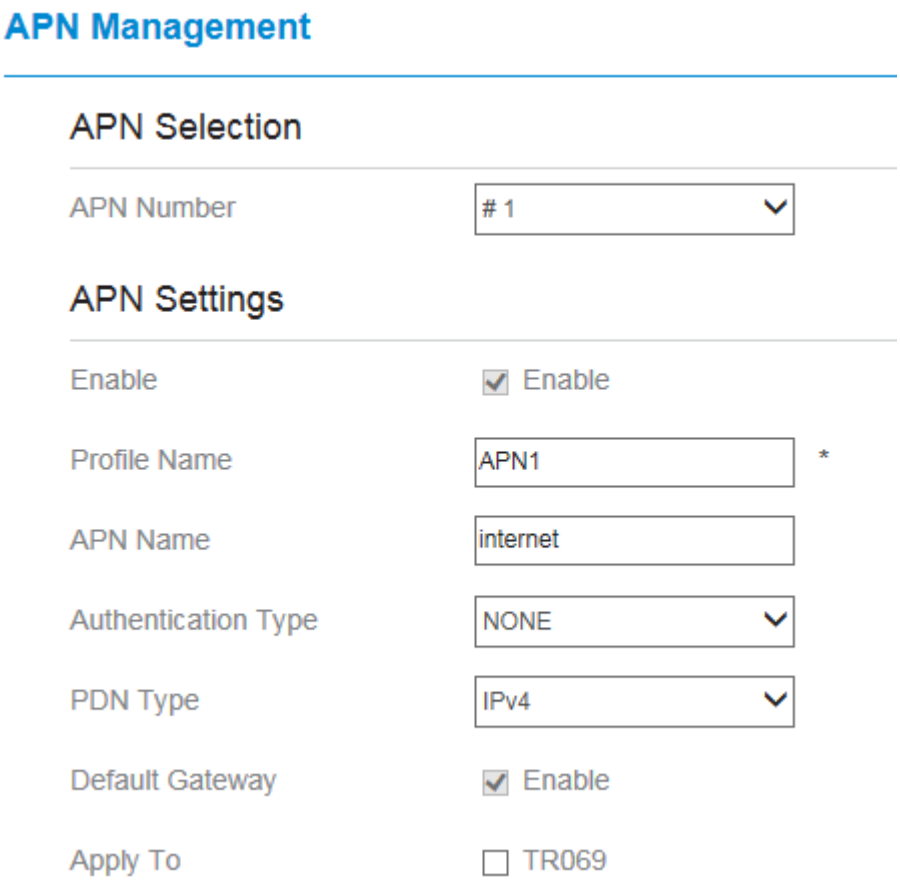
Obrázek 6-2

6.3 Správa přístupových bodů (APN)

6.3.1 Správa přístupových bodů v režimu NAT

Pro nastavení přístupových bodů v režimu NAT proveďte následující kroky:

1. Přejděte do **Settings** (Nastavení) > **Network** (Síť) > **APN Management** (Správa přístupových bodů).
2. V oblasti **APN Management** (Správa přístupových bodů) bude možné provést nastavení jednotlivých AP.
3. Zvolte požadované číslo přístupového bodu (**APN Number**).
4. V oblasti **APN Settings** můžete dále nastavit dílčí parametry přístupového bodu, jako je zapnutí/vypnutí, název, uživatelské jméno, heslo apod.
5. Vyberte z rozbalovacího seznamu **typ PDN**, např. IPv4, IPv6 nebo IPv4v6.
6. Zaškrtněte pole Enable u položky **Default Gateway**, chcete-li přístupový bod použít jako výchozí bránu.
7. Zaškrtněte pole **Apply To**, chcete-li daný přístupový bod použít pro konkrétní zařízení pomocí protokolu TR069.
8. Klikněte na tlačítko **Submit** (Uložit). Viz obrázek 6-9.



Obrázek 6-9

6.3.2 Seznam přístupových bodů

Seznam přístupových bodů zobrazíte následujícími kroky:

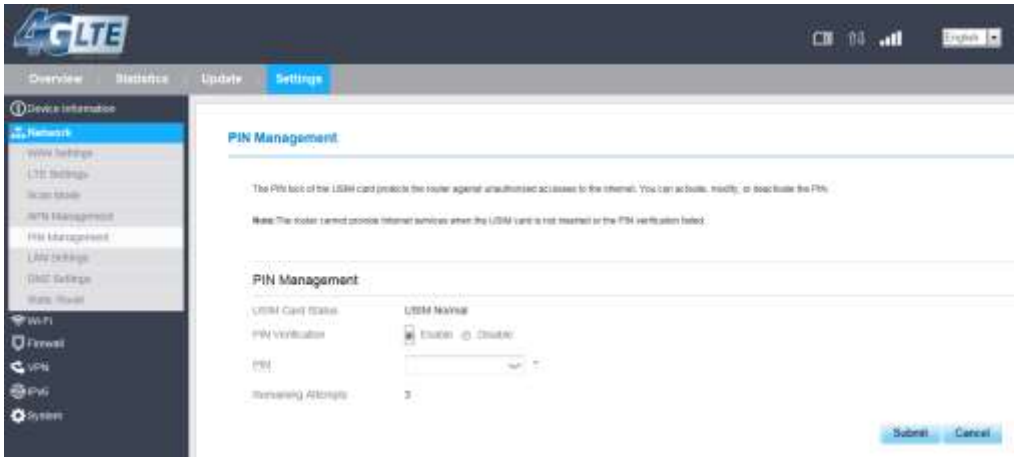
1. Přejděte do **Settings** (Nastavení) > **Network** (Síť) > **APN Management** (Správa přístupových bodů).
2. V oblasti **APN List** (Seznam přístupových bodů) bude zobrazen seznam jednotlivých přístupových bodů. Viz obrázek 6-10.

Obrázek 6-10

6.4 Správa kódu PIN

Na obrazovce PIN Management se nachází následující položky pro správu ověření pomocí kódu PIN:

1. Zapnutí nebo vypnutí ověření prostřednictvím kódu PIN.
2. Ověřit kód PIN.
3. Změnit kód PIN.
4. Nastavit automatické ověření prostřednictvím kódu PIN. Viz obrázek 6-11.



Obrázek 6-11

6.4.1 Zobrazení stavu karty USIM

Pro zobrazení stavu karty USIM proveďte následující kroky:

1. Přejděte do **Settings** (Nastavení) > **Network** (Síť) > **PIN Management** (Správa PIN).
2. Stav karty USIM bude zobrazen v poli **USIM Card Status**.

6.4.2 Zapnutí ověření kódem PIN

Pro aktivaci ověřování pomocí kódu PIN proveďte následující kroky:

1. Přejděte do **Settings** (Nastavení) > **Network** (Síť) > **PIN Management** (Správa PIN).
2. Označte volbu **Enable** (Povolit) u položky **PIN Verification** (Ověření kódem PIN).
3. Zadejte kód PIN (4–8 číslic) do pole **Enter PIN**.
4. Klikněte na tlačítko **Submit** (Uložit).

6.4.3 Vypnutí ověření kódem PIN

Pro vypnutí ověřování pomocí kódu PIN proveďte následující kroky:

1. Přejděte do **Settings** (Nastavení) > **Network** (Síť) > **PIN Management** (Správa PIN).
2. Označte volbu **Disable** (Vypnout) u položky **PIN Verification** (Ověření kódem PIN).
3. Zadejte kód PIN (4–8 číslic) do pole **Enter PIN**.

4. Klikněte na tlačítko **Submit** (Uložit).

6.4.4 Ověření kódu PIN

Pokud je ověření kódem PIN zapnuto, a zatím nedošlo k zadání správného kódu PIN, je zapotřebí jeho ověření. Pro ověření kódu PIN proveďte následující kroky:

1. Přejděte do **Settings** (Nastavení) > **Network** (Síť) > **PIN Management** (Správa PIN).
2. Zadejte kód PIN (4–8 číslic) do pole **PIN**.
3. Klikněte na tlačítko **Submit** (Uložit).

6.4.5 Změna kódu PIN

Kód PIN lze změnit pouze v případě, že je ověřování kódem PIN zapnuto a byl zadán správný kód PIN.

Pro změnu kódu PIN proveďte následující kroky:

1. Přejděte do nastavení **Network** (Síť) > **PIN Management** (Správa PIN).
2. Označte volbu **Enable** (Povolit) u položky PIN Verification (Ověření kódem PIN).
3. Nastavte položku **Change PIN** (Změna kódu PIN) na **Enable** (Zapnuto).
4. Zadejte aktuální kód PIN (4–8 číslic) do pole **PIN**.
5. Zadejte nový kód PIN (4–8 číslic) do pole **New PIN**.
6. Pro potvrzení opakujte zadání kódu PIN do pole **Confirm PIN**.
7. Klikněte na tlačítko **Submit** (Uložit).

6.4.6 Nastavení automatického ověření kódu PIN

Automatické ověření kódu PIN lze zapnout nebo vypnout. Pokud bude automatické ověřování zapnuto, bude CPE po každém restartování vyžadovat zadání kódu PIN. Tuto funkci lze zapnout pouze v případě, že je ověřování kódem PIN zapnuto a byl zadán správný kód PIN.

Pro aktivaci automatického ověřování kódu PIN proveďte následující kroky:

1. Přejděte do nabídky **Settings** (Nastavení) > **Network** (Síť) > **PIN Management** (Správa PIN).
2. Označte volbu **Enable** (Povolit) u položky PIN Verification (Ověření kódem PIN).
3. Označte volbu **Enable** také u položky Remember my PIN (Zapamatovat kód PIN).
4. Klikněte na tlačítko **Submit** (Uložit).

6.4.7 Ověření kódu PUK

Pokud je ověřování kódem PIN zapnuto, a uživatel zadá třikrát po sobě nesprávný kód PIN, dojde k jeho uzamčení. V tomto případě bude zapotřebí zadat pro odemčení správný kód PUK.

Pro ověření kódu PUK proveďte následující kroky:

1. Přejděte do nastavení **Network** (Síť) > **PIN Management** (Správa PIN).
2. Zadejte kód PUK do pole **PUK**.
3. Zadejte nový kód PIN do pole **New PIN**.
4. Pro potvrzení opakujte zadání kódu PIN do pole **Confirm PIN**.
5. Klikněte na tlačítko **Submit** (Uložit).

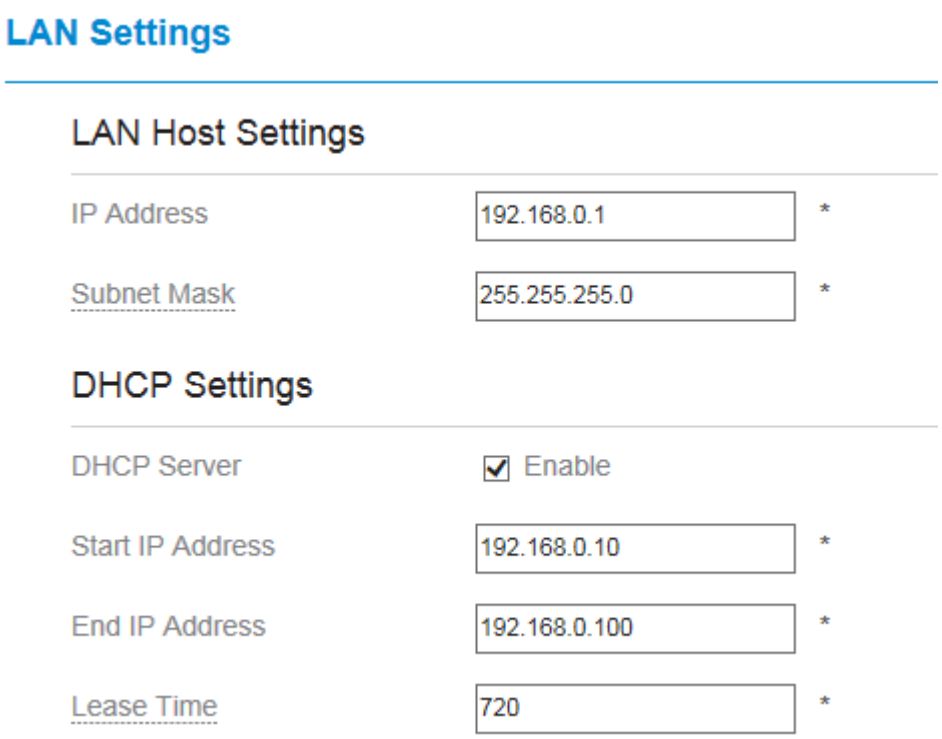
6.5 Nastavení místní sítě (LAN)

6.5.1 Nastavení parametrů hostitele v místní síti LAN

Ve výchozím nastavení je IP adresa hostitele 192.168.0.1 a maska podsítě 255.255.255.0. Adresu IP hostitele je možné libovolně změnit na adresu, která pro vás bude snadno zapamatovatelná. Je třeba se pouze ujistit, že zadaná IP adresa bude ve vaší síti unikátní. Po změně IP adresy vašeho CPE bude webové rozhraní pro správu k dispozici pod novou IP adresou.
Pro změnu IP adresy CPE proveďte následující kroky:

1. Přejděte do nabídky **Settings** (Nastavení) **> Network** (Síť) **> LAN Settings** (Nastavení LAN).
2. V oblasti **LAN Host Settings** (Nastavení hostitele LAN) zadejte IP adresu a masku podsítě.
3. V oblasti **DHCP Setting** (Nastavení DHCP) zapněte server DHCP zaškrtnutím položky **Enable**.

   ⚠ Nastavení DHCP je dostupné pouze v režimu NAT.
4. Klikněte na tlačítko **Submit** (Uložit). Viz obrázek 6-13.



Obrázek 6-13

6.5.2 Konfigurace DHCP serveru

DHCP umožňuje jednotlivým klientským zařízením po zapnutí automaticky získat konfiguraci TCP/IP ze serveru. Vaše CPE může sloužit jako DHCP server, tuto funkci však je možné vypnout. V případě, že je DHCP server tohoto CPE aktivní, bude automaticky přidělovat konfiguraci TCP/IP jednotlivým klientským zařízením v síti LAN, které tuto funkci podporují. Pokud funkci DHCP vypnete, je zapotřebí do místní sítě LAN zapojit jiný server DHCP, případně nakonfigurovat každé klientské zařízení v síti ručně.

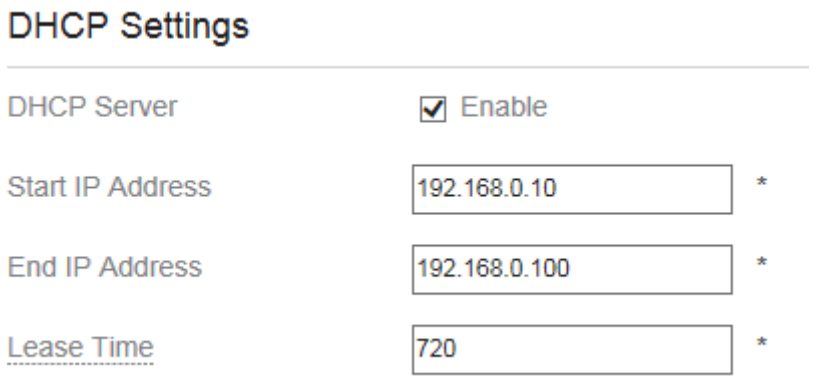
Pro změnu nastavení funkce DHCP proveďte následující kroky:

1. Přejděte do nabídky **Settings** (Nastavení) **> Network** (Síť) **> LAN Settings** (Nastavení LAN).
2. Zapněte server DHCP zaškrtnutím pole **Enable**.
3. Zadejte počátek rozsahu přidělovaných IP adres do pole **Start IP**.

   Tato adresa se musí lišit od IP adresy zadané v poli **LAN Host Settings** (Nastavení hostitele LAN), avšak je nutné, aby byly ve stejném síťovém segmentu.
4. Zadejte konec rozsahu přidělovaných IP adres do pole **End IP**.

   Tato adresa se musí lišit od IP adresy zadané v poli **LAN Host Settings** (Nastavení hostitele LAN), avšak je nutné, aby byly ve stejném síťovém segmentu.
5. Nastavte dobu zapůjčení do pole **Lease time**.

   Dobu zapůjčení lze nastavit v rozsahu 2–1440 minut. Doporučujeme výchozí hodnotu zachovat.
6. Klikněte na tlačítko **Submit** (Uložit). Viz obrázek 6-14.



Obrázek 6-14

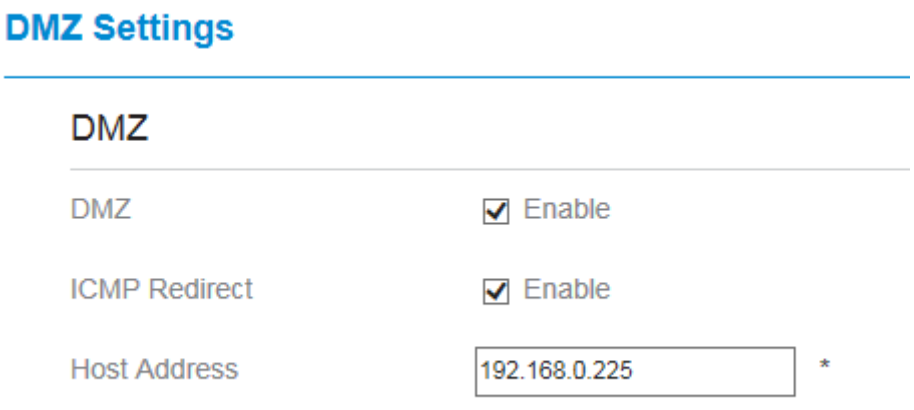
6.6Nastavení neutrální zóny DMZ

Pokud je aktivní funkce neutrální zóny (DMZ), budou pakety odeslané ze sítě WAN před zahozením branou firewall přeposlány na zadanou IP adresu v síti LAN.

Pro neutrální zóny (DMZ) proveďte následující kroky:

1. Přejděte do nastavení **Settings** (Nastavení) > **Network** (Síť) > **DMZ Settings (Nastavení DMZ).**
2. Zapněte funkci neutrální zóny zaškrtnutím pole **Enable** u položky DMZ.
3. Volitelně můžete zapnout také přesměrování zpráv ICMP zaškrtnutím pole **Enable** u položky **ICMP Redirect**.
4. Zadejte adresu hostitele do pole **Host address**.

   Tato adresa se musí lišit od IP adresy zadané v poli **LAN Host Settings** (Nastavení hostitele LAN), avšak je nutné, aby byly ve stejném síťovém segmentu.
5. Klikněte na tlačítko **Submit** (Uložit). Viz obrázek 6-15.



Obrázek 6-15

7 Bezdrátová síť Wi-Fi

7.1 Přehled o stavu WLAN

Přehled o stavu sítě WAN získáte následujícími kroky:

1. Klikněte na záložku **Overview** (Přehled).
2. V oblasti **WAN Status** budou zobrazeny dílčí informace o stavu sítě WAN. Viz obrázek 7-1.

Obrázek 7-1

7.2Nastavení sítě WLAN

Tato funkce umožňuje nastavení dílčích parametrů sítě Wi-Fi.

7.2.1 Obecné nastavení

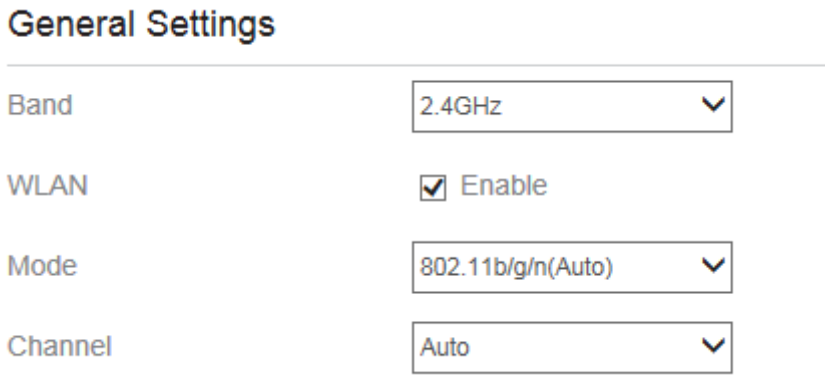
Pro změnu obecných nastavení sítě Wi-Fi proveďte následující kroky:

1. Přejděte do nabídky **Wi-Fi > Wi-Fi Settings** (Nastavení Wi-Fi).
2. V oblasti **General Settings** (Obecné nastavení) zapněte síť Wi-Fi zaškrtnutím pole **Enable**.
3. Pomocí rozbalovací nabídky **Mode** vyberte režim bezdrátové sítě podle popisu v následující tabulce:

Hodnota parametru	**Popis**
802.11 a/n/ac	Klientské zařízení Wi-Fi se bude moci připojit k CPE pomocí režimu 802.11a, 802.11n nebo 802.11ac na frekvenci 5 GHz ISM. Pokud vaše zařízení podporuje protokol 802.11ac, doporučujeme jej kvůli lepší kvalitě připojení používat.

802.11b/g/n	Klientské zařízení Wi-Fi se bude moci připojit k CPE pomocí režimu 802.11b, 802.11g nebo 802.11n. V případě, že bude klientské zařízení připojeno k CPE v režimu 802.11n, je vyžadováno šifrování AES (Advanced Encryption Standard).
802.11b/g	Klientské zařízení Wi-Fi se bude moci připojit k CPE pomocí režimu 802.11b nebo 802.11g.
802.11b	Klientské zařízení Wi-Fi se bude moci připojit k CPE pomocí režimu 802.11b.
802.11g	Klientské zařízení Wi-Fi se bude moci připojit k CPE pomocí režimu nebo 802.11g.

4. Pomocí rozbalovací nabídky **Channel** zvolte číslo kanálu – od 1 do 11 v případě použití frekvenčního pásma 2,4 GHz a od 40 do 165 při použití pásma 5 GHz.
5. Klikněte na tlačítko **Submit** (Uložit). Viz obrázek 7-2.



Obrázek 7-2

7.3Nastavení profilu SSID

Po konfiguraci modemu v oblasti **SSID Profile** (Profil SSID) se klientské zařízení Wi-Fi připojí k CPE na základě přednastavených pravidel, které zvýší zabezpečení přístupu.

Pro nastavení profilu SSID modemu na stránce **SSID Profile** postupujte podle následujících kroků:

1. Přejděte do nabídky **Wi-Fi > Wi-Fi Settings** (Nastavení Wi-Fi).
2. Zadejte požadovaný název sítě **SSID**.

   Název sítě SSID může obsahovat 1 až 32 znaků ASCII. Nemůže se jednat o prázdný řetězec a poslední znak nesmí být prázdný (např. mezera). Součástí SSID dále nemohou být následující speciální znaky: / ' = " \ &

   Klientské zařízení Wi-Fi se k CPE připojí pomocí daného názvu sítě SSID.
3. Zadejte maximální počet připojených zařízení do pole **Maximum number of devices**.

   Tento parametr vyjadřuje maximální počet klientských zařízení, které mohou být připojeny současně.

   Celkem může být k CPE připojeno až 32 zařízení.
4. Můžete skrýt název sítě zaškrtnutím pole **Enable** u položky **Hide SSID broadcast**.

Pokud bude název sítě skrytý, nebudou klientská zařízení schopna rozpoznat informace o síti.

5. Můžete rovněž aktivovat izolaci přístupových bodů zaškrtnutím pole **Enable** u položky **AP isolation**.

   Klientská zařízení se budou moci připojit k CPE, avšak vzájemná komunikace nebude možná.

6. Pomocí rozbalovací nabídky **Security** vyberte požadovanou úroveň zabezpečení.

   Pokud bude položka **Security** (Zabezpečení) nastavena na **NONE (nedoporučujeme)**, klientským zařízením Wi-Fi bude umožněno přímé připojení k CPE. Tato úroveň zabezpečení je velmi nedostačující.

   Pokud bude položka **Security** (Zabezpečení) nastavena na WEP, bude klientským zařízením umožněno připojení k síti Wi-Fi po ověření klíče WEP.

   Pokud bude položka **Security** (Zabezpečení) nastavena na **WPA-PSK**, bude klientským zařízením umožněno připojení k síti Wi-Fi po ověření klíče WPA-PSK.

   Pokud bude položka **Security** (Zabezpečení) nastavena na **WPA2-PSK**, bude klientským zařízením umožněno připojení k síti Wi-Fi po ověření klíče WPA2-PSK. Toto nastavení doporučujeme z důvodu maximální míry zabezpečení.

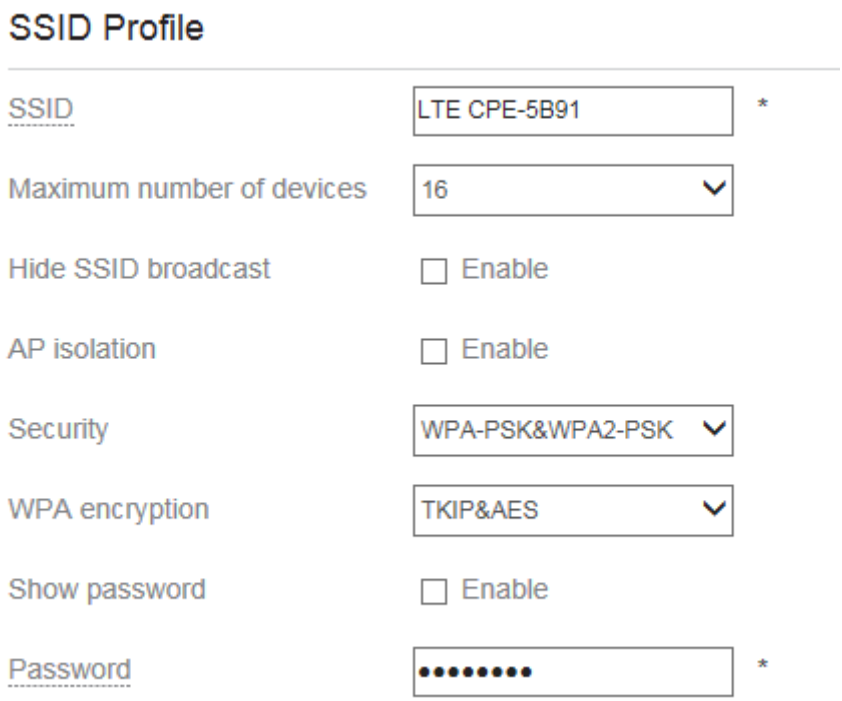
   Pokud bude položka **Security** (Zabezpečení) nastavena na **WPA-PSK & WPA2-PSK**, bude klientským zařízením umožněno připojení k síti Wi-Fi po ověření v režimu WPA-PSK nebo WPA2-PSK.

7. Nastavte režim šifrování.

Režim šifrování	Nastavení	Popis
WEP	Režim ověření	● **Sdílené ověření:** Klientské zařízení se připojí k CPE ve sdíleném režimu ověření. ● **Otevřené ověření:** Klientské zařízení se připojí k CPE v otevřeném režimu ověření. ● **Obě:** Klientské zařízení se připojí k CPE ve sdíleném nebo otevřeném režimu ověření.
	Délka hesla	● **128 bitů**: Do textových polí pro zadání přístupového hesla **Key 1** až **Key 4** lze zadat 13 znaků ASCII nebo 26 hexadecimálních znaků. ● **64 bitů:** Do textových polí pro zadání přístupového hesla **Key 1** až **Key 4** lze zadat 5 znaků ASCII nebo 10 hexadecimálních znaků.
	Index aktuálního hesla	Tuto hodnotu lze nastavit na **1, 2, 3** nebo **4**. Po zvolení požadovaného indexu bude platit heslo s daným číslem.
WPA-PSK	WPA-PSK	Zadat lze 8–63 znaků ASCII nebo 8–64 hexadecimálních znaků.
	Šifrování WPA	Tuto položku je možné nastavit na **TKIP+AES**, **AES** nebo **TKIP**.
WPA2-PSK (doporučujeme)	WPA-PSK	Zadat lze 8–63 znaků ASCII nebo 8–64 hexadecimálních znaků.
	Šifrování WPA	Tuto položku je možné nastavit na **TKIP+AES**, **AES**

		nebo **TKIP**.
WPA-PSK & WPA2-PSK	WPA-PSK	Zadat lze 8–63 znaků ASCII nebo 8–64 hexadecimálních znaků.
	Šifrování WPA	Tuto položku je možné nastavit na **TKIP+AES**, **AES** nebo **TKIP**.

8. Klikněte na tlačítko **Submit** (Uložit). Viz obrázek 7-3.



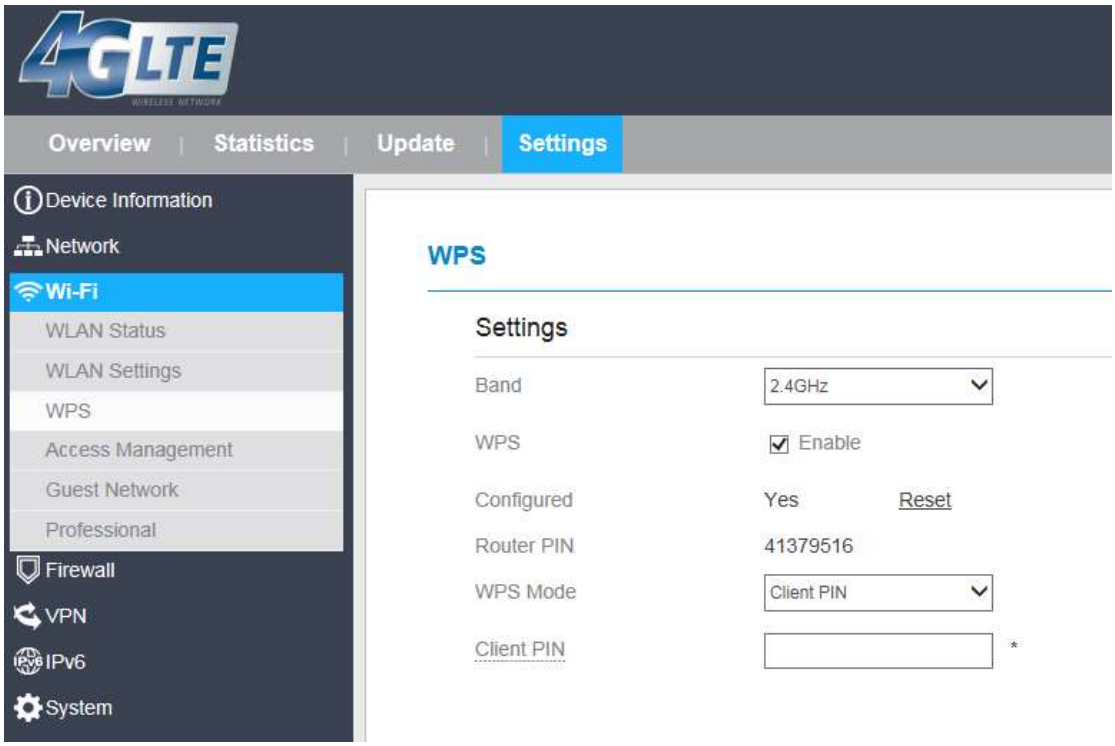
Obrázek 7-1

7.4WPS

Wi-Fi Protected Setup (WPS) je síťové zabezpečení bezpečnostní standard pro vytvoření zabezpečené domácí bezdrátové sítě.

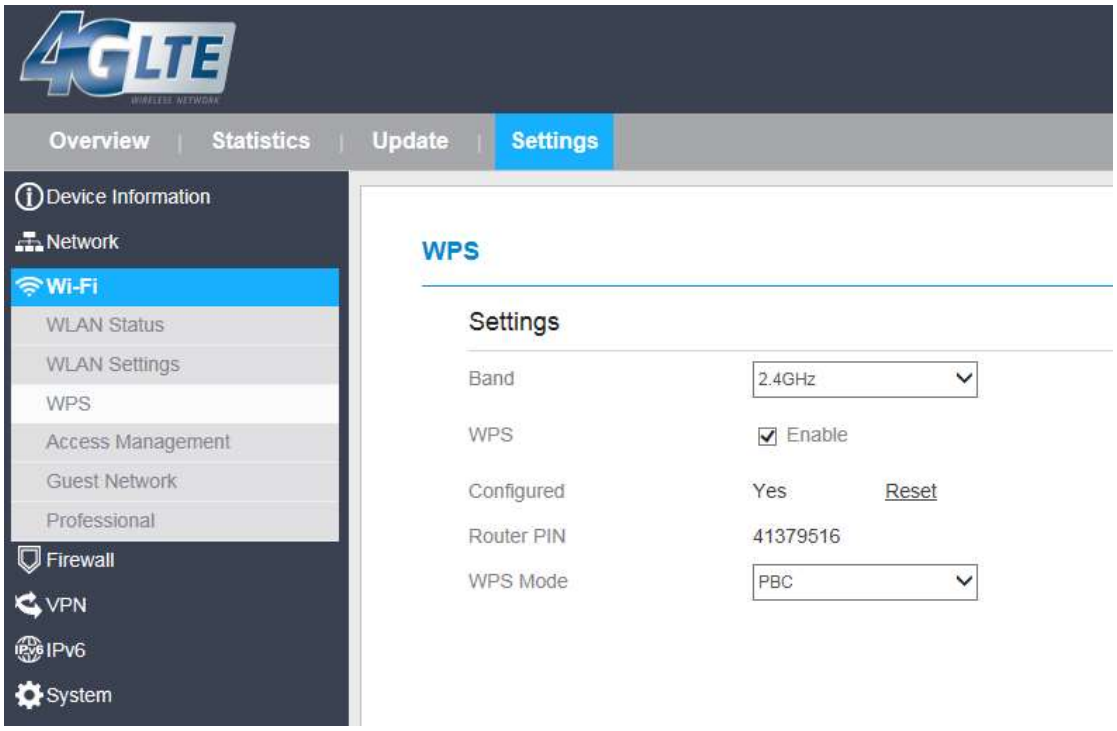
Pro nastavení WPS proveďte následující kroky:

1. Přejděte to nabídky **Wi-Fi** > **WPS**.
2. Zapněte funkci **WPS** zaškrtnutím pole **Enable**.
3. V rozbalovací nabídce WPS Mode (režim WPS) vyberte možnost **Client PIN** (Ověření kódem PIN).
4. Zadejte do prázdného pole kód PIN. Viz obrázek 7-4.



Obrázek 7-4

5. V rozbalovací nabídce WPS Mode (režim WPS) vyberte možnost **PBC**.
6. Klikněte na tlačítko **Submit** (Uložit). Viz obrázek 7-5.



Obrázek 7-5

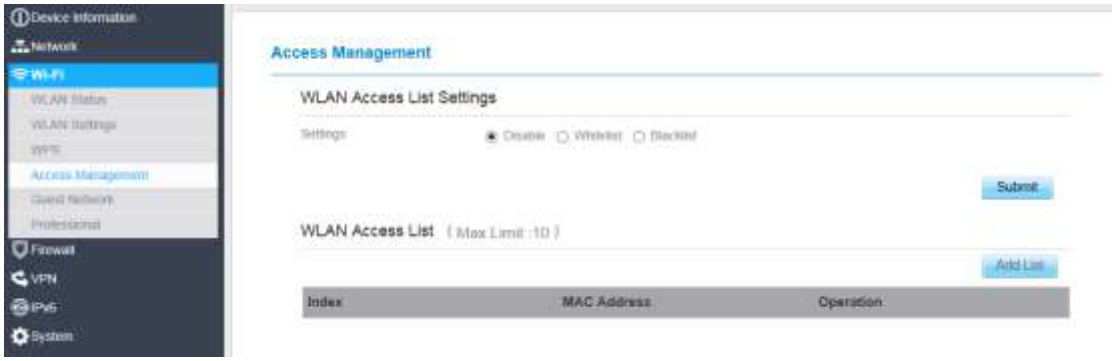
7.5Řízení přístupu

7.5.1 Nastavení přístupové politiky

Tato funkce umožňuje nastavení přístupové politiky k CPE pro jednotlivé bezdrátové sítě podle SSID.

Pro změnu nastavení řízení přístupu podle adresy MAC proveďte následující kroky:

1. Přejděte do nabídky **Wi-Fi** > **Access Management** (Řízení přístupu).
2. Vyberte požadovaný režim řízení přístupu v oblasti **WLAN Access List Settings**.
   Dostupné režimy jsou **Disable** (Vypnuto), **Blacklist** (Černá listina) nebo **Whitelist** (Bílá listina).
   - Pokud je režim nastaven na **Disable** (Vypnuto), nebudou mít omezení přístupu žádný účinek.
   - Pokud je režim nastaven na **Blacklist** (Černá listina), budou se k CPE moci připojit všechna zařízení, která nejsou na černé listině.
   - Pokud je režim nastaven na **Whitelist** (Bílá listina), budou se k CPE moci připojit pouze zařízení, která jsou na bílé listině.
3. Klikněte na tlačítko **Submit** (Uložit). Viz obrázek 7-6.



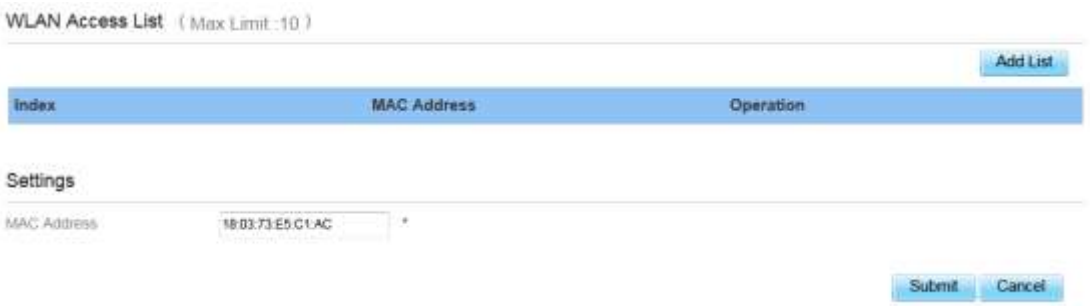
Obrázek 7-6

7.5.2 Správa seznamu zařízení s přístupem k síti Wi-Fi

Tato funkce umožňuje nastavení přístupové politiky na základě MAC adresy jednotlivých zařízení.

Pro přidání zařízení na seznam postupujte podle následujících kroků:

1. Přejděte do nabídky **Wi-Fi** > **Access Management** (Řízení přístupu).
2. Klikněte na tlačítko **Add** (Přidat).
3. Zadejte adresu zařízení do pole **MAC Address**.
4. Klikněte na tlačítko **Submit** (Uložit). Viz obrázek 7-7.



Obrázek 7-7

Pro úpravu položky ze seznamu postupujte podle následujících kroků:

1. Přejděte do nabídky **Wi-Fi** > **Access Management** (Řízení přístupu).
2. Klikněte na tlačítko **Edit MAC List**.
3. Zvolte záznam, který si přejete upravit, a klikněte na tlačítko **Edit**.
4. Zadejte adresu zařízení do pole **MAC Address**.
5. Zaškrtnutím pole **Enable** u příslušné MAC adresy aktivujete její přístup k síťovému SSID.
6. Klikněte na tlačítko **Submit** (Uložit). Viz obrázek 7-8.

Obrázek 7-8

Pro odstranění položky ze seznamu postupujte podle následujících kroků:

1. Přejděte do nabídky **Wi-Fi** > **Access Management** (Řízení přístupu).
2. Zvolte záznam, který si přejete odstranit, a klikněte na tlačítko **Delete**. Viz obrázek 7-9.

Obrázek 7-9

7.6Síť pro hosty

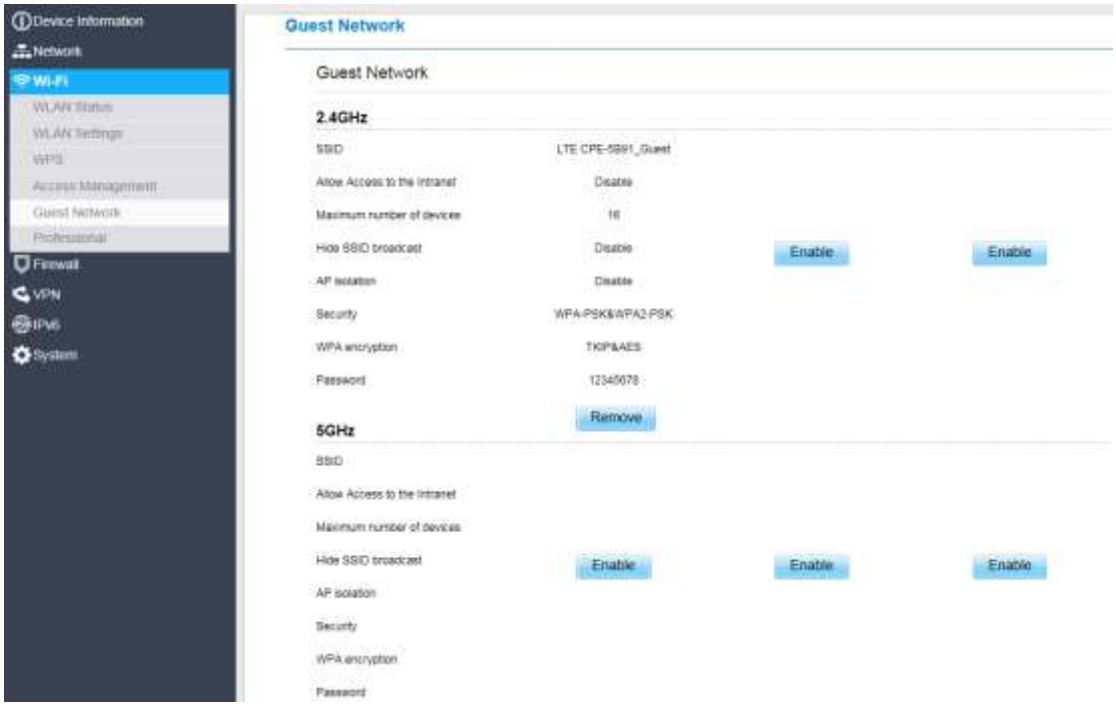
7.6.1 Síť pro hosty

Tato funkce slouží pro vytvoření dočasné a oddělené sítě pro hosty.

Pro vytvoření sítě pro hosty proveďte následující kroky:

1. Přejděte do nabídky **Wi-Fi > Guest Network** (Síť pro hosty).

2. V oblasti **Guest Network** (Síť pro hosty) aktivujte síť zaškrtnutím pole **Enable**. Viz obrázek 7-10.



Obrázek 7-10

7.7 Profesionální nastavení

Toto nastavení slouží pro výběr regionu, ve kterém se modem nachází.

1. Přejděte to nabídky **Wi-Fi** > **Professional** (Profesionální nastavení).
2. Z rozbalovací nabídky **Region** vyberte zemi, ve které se modem nachází. K dispozici je **China** (Čína)**, France** (Francie)**, United States** (Spojené státy)**, Singapore** (Singapur) a **Australia** (Austrálie).
3. Klikněte na tlačítko **Submit** (Uložit). Viz obrázek 7-11.

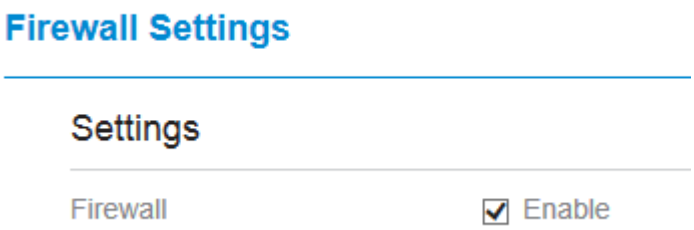
Obrázek 7-11

8 Brána firewall

8.1 Nastavení brány firewall

Pro zapnutí brány firewall proveďte následující kroky:

1. Přejděte do nabídky **Settings** (Nastavení) > **Firewall** (Brána firewall) > **Firewall Settings** (Nastavení brány firewall).
2. Bránu firewall zapnete zaškrtnutím pole **Enable**.
3. Klikněte na tlačítko **Submit** (Uložit). Viz obrázek 8-1.



Obrázek 8-1

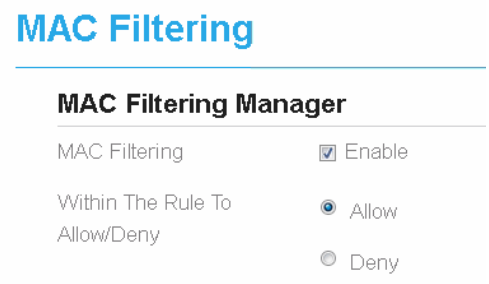
8.2 Filtrování adres MAC

Tato stránka umožňuje nastavení pravidel filtrování podle adres MAC.

8.2.1 Zapnutí filtrování adres MAC

Pro zapnutí filtrování adres MAC proveďte následující kroky:

1. Přejděte do nabídky **Settings** (Nastavení) > **Firewall** (Brána firewall) > **MAC Filtering** (Filtrování adres MAC).
2. Zaškrtněte položku **Enable** pro zapnutí filtrování adres MAC.
3. Klikněte na tlačítko **Submit** (Uložit). Viz obrázek 8-2.

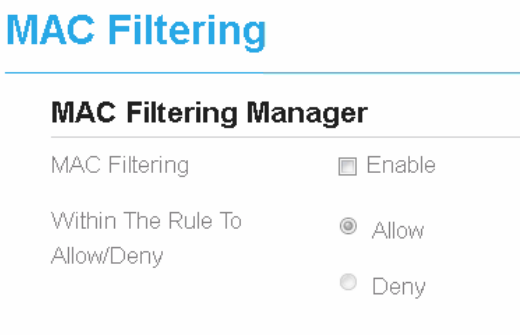


Obrázek 8-2

8.2.2 Vypnutí filtrování adres MAC

Pro vypnutí filtrování adres MAC proveďte následující kroky:

1. Přejděte do nabídky **Settings** (Nastavení) > **Firewall** (Brána firewall) > **MAC Filtering** (Filtrování adres MAC).
2. Odškrtněte položku **Enable** pro vypnutí filtrování adres MAC.
3. Klikněte na tlačítko **Submit** (Uložit). Viz obrázek 8-3.

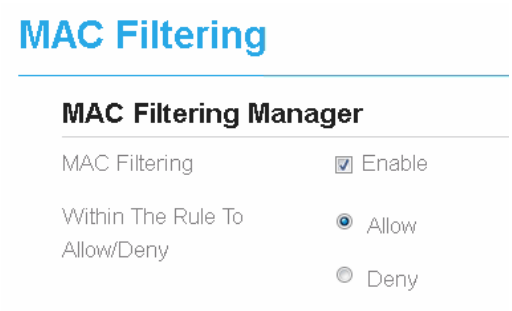


Obrázek 8-3

8.2.3 Nastavení pravidla povolení přístupu

Pro nastavení pravidla povolení přístupu proveďte následující kroky:

1. Přejděte do nabídky **Settings** (Nastavení) > **Firewall** (Brána firewall) > **MAC Filtering** (Filtrování adres MAC).
2. Zaškrtněte položku **Allow access network** (Povolit přístup k síti).
3. Klikněte na tlačítko **Submit** (Uložit). Viz obrázek 8-4.

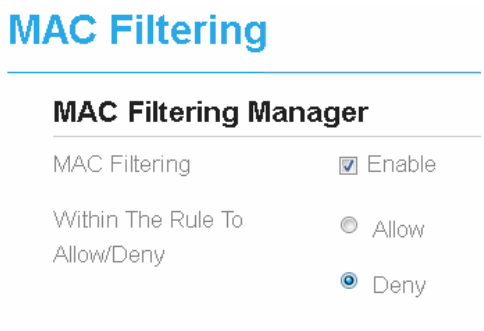


Obrázek 8-4

8.2.4 Nastavení pravidla odepření přístupu

Pro nastavení pravidla odepření přístupu proveďte následující kroky:

1. Přejděte do nabídky **Settings** (Nastavení) > **Firewall** (Brána firewall) > **MAC Filtering** (Filtrování adres MAC).
2. Zaškrtněte položku **Deny access network** (Odepřít přístup k síti).
3. Klikněte na tlačítko **Submit** (Uložit). Viz obrázek 8-5.

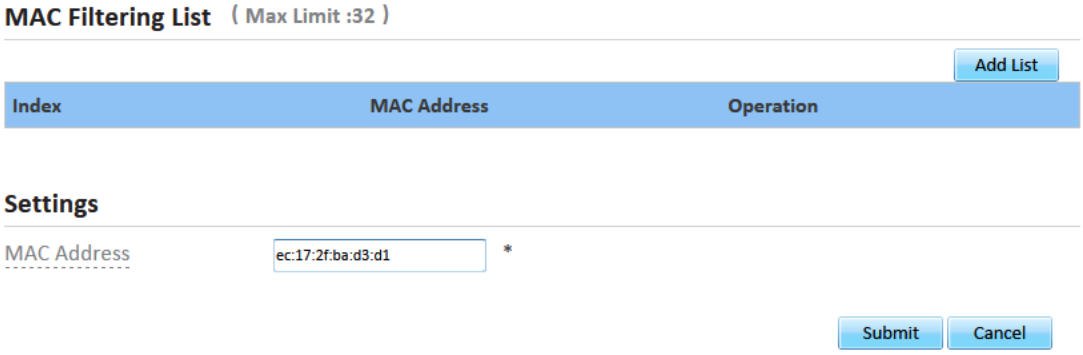


Obrázek 8-5

8.2.5 Přidání pravidla filtrování adres MAC

Pro přidání pravidla filtrování adres MAC proveďte následující kroky:

1. Přejděte do nabídky **Settings** (Nastavení) > **Firewall** (Brána firewall) > **MAC Filtering** (Filtrování adres MAC).
2. Klikněte na tlačítko **Add list** (Přidat seznam).
3. Zadejte adresu zařízení do pole **MAC Address**.
4. Klikněte na tlačítko **Submit** (Uložit). Viz obrázek 8-6.

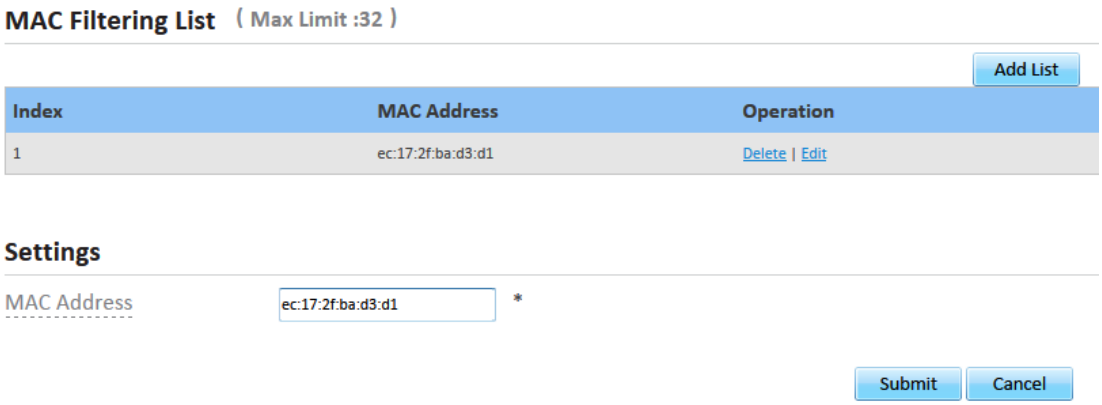


Obrázek 8-6

8.2.6 Upravení pravidla filtrování adres MAC

Pro upravení pravidla filtrování adres MAC proveďte následující kroky:

1. Přejděte do nabídky **Settings** (Nastavení) > **Firewall** (Brána firewall) > **MAC Filtering** (Filtrování adres MAC).
2. Zvolte záznam, který si přejete upravit, a klikněte na tlačítko **Edit**.
3. Zadejte adresu zařízení do pole **MAC Address**.
4. Klikněte na tlačítko **Submit** (Uložit). Viz obrázek 8-7.

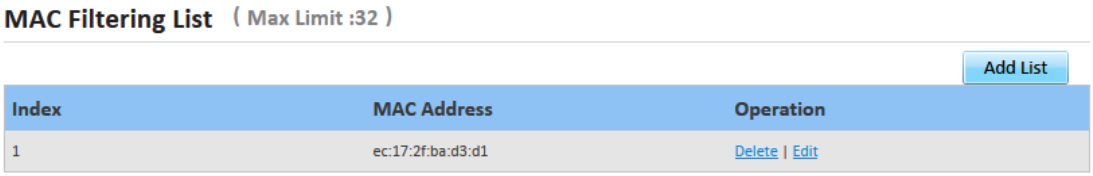


Obrázek 8-7

8.2.7 Odstranění pravidla filtrování adres MAC

Pro odstranění pravidla filtrování adres MAC proveďte následující kroky:

1. Přejděte do nabídky **Settings** (Nastavení) > **Firewall** (Brána firewall) > **MAC Filtering** (Filtrování adres MAC).
2. Zvolte záznam, který si přejete odstranit, a klikněte na tlačítko **Delete**. Viz obrázek 8-8.



Obrázek 8-8

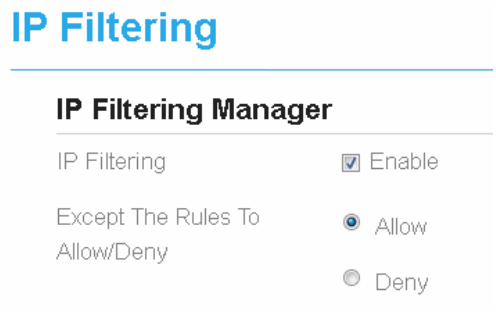
8.3 Filtrování IP adres

Datový tok je filtrován na základě IP adres. Tato stránka umožňuje nastavení pravidel filtrování podle IP adres.

8.3.1 Zapnutí filtrování IP adres

Pro zapnutí filtrování IP adres proveďte následující kroky:

1. Přejděte do nabídky **Settings** (Nastavení) > **Firewall** (Brána firewall) > **IP Filtering** (Filtrování IP adres).
2. Zaškrtněte položku **Enable** pro zapnutí filtrování IP adres.
3. Klikněte na tlačítko **Submit** (Uložit). Viz obrázek 8-9.

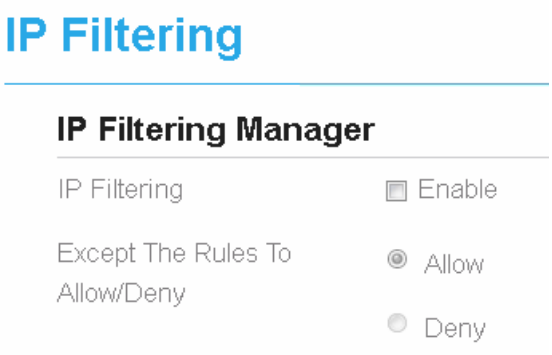


Obrázek 8-9

8.3.2 Vypnutí filtrování IP adres

Pro vypnutí filtrování IP adres proveďte následující kroky:

1. Přejděte do nabídky **Settings** (Nastavení) > **Firewall** (Brána firewall) > **IP Filtering** (Filtrování IP adres).
2. Odškrtněte položku **Enable** pro vypnutí filtrování IP adres.
3. Klikněte na tlačítko **Submit** (Uložit). Viz obrázek 8-10.

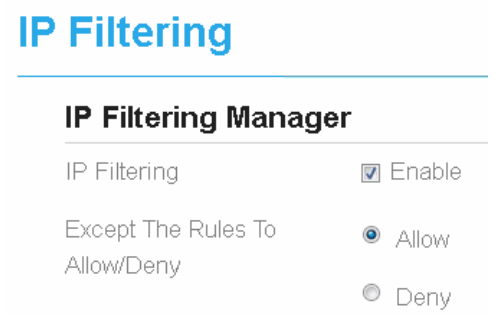


Obrázek 8-10

8.3.3 Nastavení povolení přístupu k síti mimo pravidla

Pro povolení přístupu k síti postupujte podle následujících kroků:

1. Přejděte do nabídky **Settings** (Nastavení) > **Firewall** (Brána firewall) > **IP Filtering** (Filtrování IP adres).
2. Zaškrtněte položku **Allow access network** (Povolení přístupu k síti) pro zapnutí pravidla.
3. Klikněte na tlačítko **Submit** (Uložit). Viz obrázek 8-11.

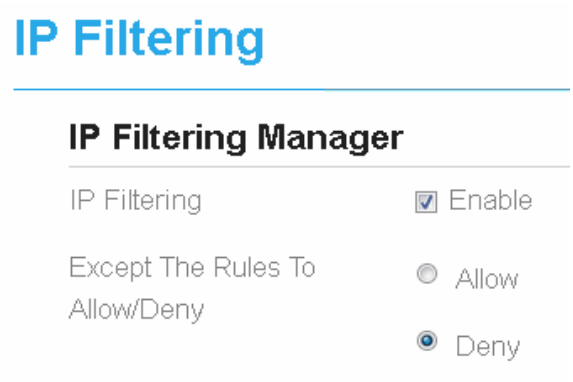


Obrázek 8-11

8.3.4 Nastavení odepření přístupu k síti mimo pravidla

Pro povolení přístupu k síti postupujte podle následujících kroků:

1. Přejděte do nabídky **Settings** (Nastavení) > **Firewall** (Brána firewall) > **IP Filtering** (Filtrování IP adres).
2. Zaškrtněte položku **Deny access network** (Odepření přístupu k síti) pro zapnutí pravidla.
3. Klikněte na tlačítko **Submit** (Uložit). Viz obrázek 8-12.

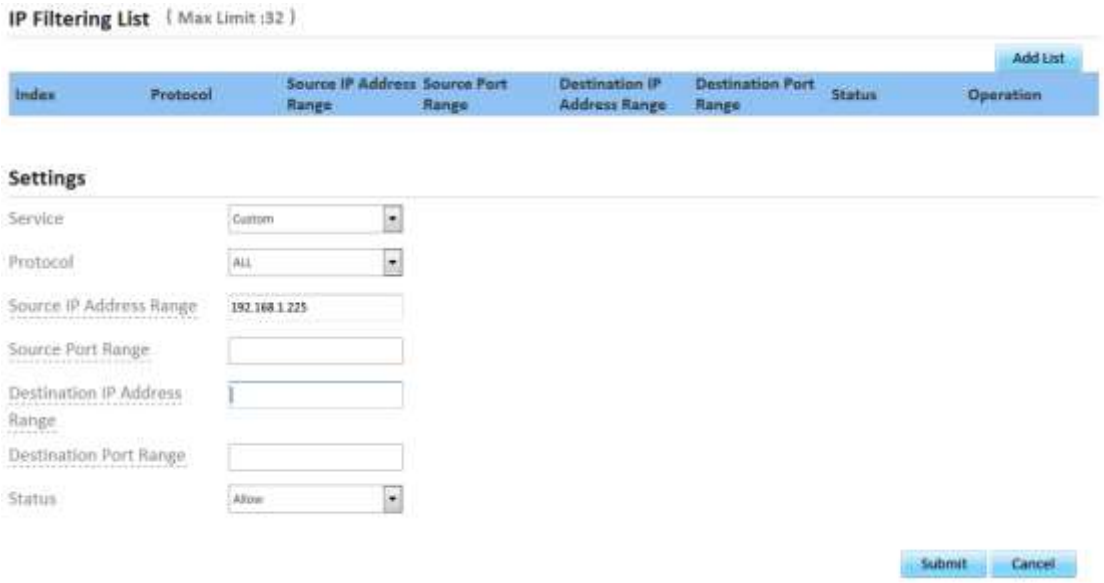


Obrázek 8-22

8.3.5 Přidání pravidla filtrování IP adres

Pro přidání pravidla filtrování IP adres proveďte následující kroky:

1. Přejděte do nabídky **Settings** (Nastavení) > **Firewall** (Brána firewall) > **IP Filtering** (Filtrování IP adres).
2. Klikněte na tlačítko **Add list** (Přidat seznam).
3. Z rozbalovací nabídky **Service** vyberte požadovanou službu.
4. Z rozbalovací nabídky **Protocol** vyberte protokol.
5. Do pole **Source IP Address Range** zadejte zdrojovou IP adresu nebo segment adresy, který si přejete filtrovat.
6. Do pole **Source Port Range** zadejte zdrojový port nebo segment portu, který si přejete filtrovat.
7. Do pole **Destination IP Address Range** zadejte cílovou IP adresu nebo segment cílové adresy, který si přejete filtrovat.
8. Do pole **Destination Port Range** zadejte cílový port nebo segment cílového portu, který si přejete filtrovat.
9. Z rozbalovací nabídky **Status** vyberte, zda chcete dané pravidlo aktivovat.
10. Klikněte na tlačítko **Submit** (Uložit). Viz obrázek 8-13.

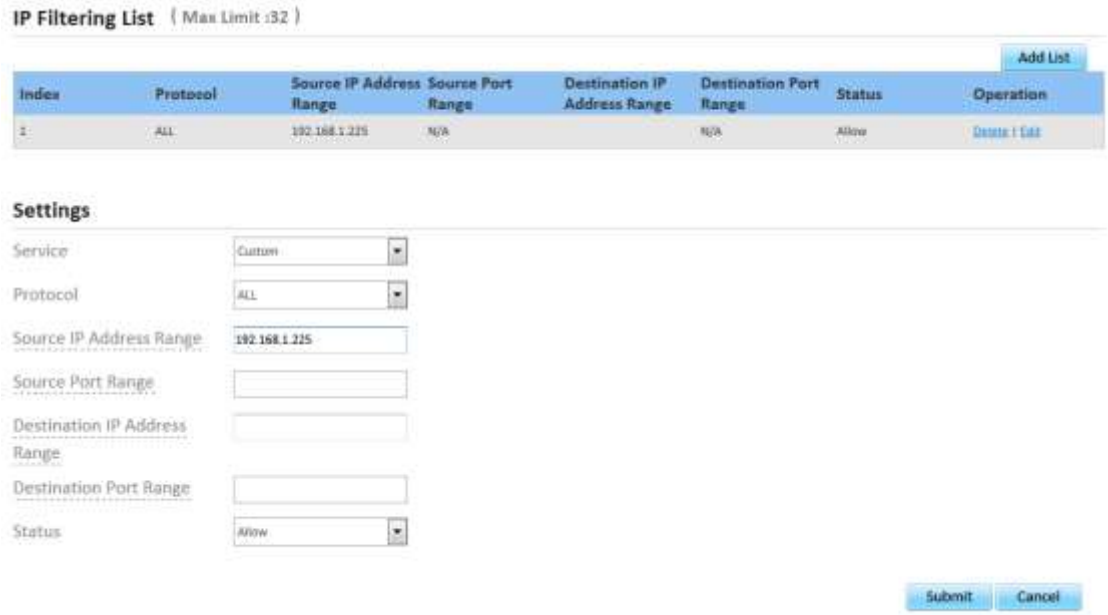


Obrázek 8-13

8.3.6 Upravení pravidla filtrování IP adres

Chcete-li změnit pravidlo filtrování IP adresy, proveďte následující kroky:

1. Přejděte do nabídky **Settings** (Nastavení) > **Firewall** (Brána firewall) > **IP Filtering** (Filtrování IP adres).
2. Zvolte pravidlo, které si přejete upravit, a klikněte na tlačítko **Edit**.
3. Opakujte kroky kroky 3 až 9 popsané v předchozí části.
4. Klikněte na tlačítko **Submit** (Uložit). Viz obrázek 8-14.



Obrázek 8-14

8.3.7 Odstranění pravidla filtrování IP adres

Chcete-li odstranit pravidlo filtrování IP adres, proveďte následující kroky:

1. Přejděte do nabídky **Settings** (Nastavení) > **Firewall** (Brána firewall) > **IP Filtering** (Filtrování IP adres).
2. Zvolte záznam, který si přejete odstranit, a klikněte na tlačítko **Delete**. Viz obrázek 8-15.

Obrázek 8-35

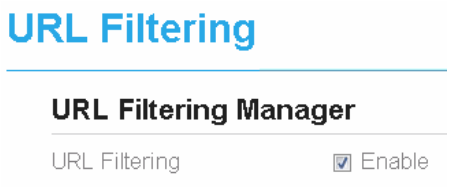
8.4 Filtrování adres URL

Datový tok je filtrován podle adresy URL. Tato stránka umožňuje nastavení pravidel filtrování podle adresy URL.

8.4.1 Zapnutí filtrování adres URL

Pro zapnutí filtrování adres URL proveďte následující kroky:

1. Přejděte do nabídky **Settings** (Nastavení) > **Firewall** (Brána firewall) > **URL Filtering** (Filtrování adres URL).
2. Zaškrtněte položku **Enable** u položky **URL Filtering** pro zapnutí filtrování adres URL.
3. Klikněte na tlačítko **Submit** (Uložit). Viz obrázek 8-16.



Obrázek 8-46

8.4.2 Vypnutí filtrování adres URL

Pro vypnutí filtrování adres URL proveďte následující kroky:

1. Přejděte do nabídky **Settings** (Nastavení) > **Firewall** (Brána firewall) > **URL Filtering** (Filtrování adres URL).
2. Odškrtněte položku **Enable** u položky **URL Filtering** pro vypnutí filtrování adres URL.
3. Klikněte na tlačítko **Submit** (Uložit). Viz obrázek 8-17.

Obrázek 8-57

8.4.3 Přidání adresy URL na seznam

Pro přidání položky na seznam filtrovaných adres URL proveďte následující kroky:

1. Přejděte do nabídky **Settings** (Nastavení) > **Firewall** (Brána firewall) > **URL Filtering** (Filtrování adres URL).
2. Klikněte na tlačítko **Add list** (Přidat seznam).
3. Zadejte adresu **URL** do stejnojmenného pole.
4. Klikněte na tlačítko **Submit** (Uložit). Viz obrázek 8-18.

Obrázek 8-68

8.4.4 Upravení adresy URL v seznamu

Chcete-li změnit pravidlo filtrování adresy URL, proveďte následující kroky:

1. Přejděte do nabídky **Settings** (Nastavení) > **Firewall** (Brána firewall) > **URL Filtering** (Filtrování adres URL).
2. Zvolte záznam, který si přejete upravit, a klikněte na tlačítko **Edit**.
3. Zadejte adresu do pole **URL**.
4. Klikněte na tlačítko **Submit** (Uložit). Viz obrázek 8-19.

Obrázek 8-79

8.4.5 Odstranění adresy URL ze seznamu

Pro odstranění adresy URL ze seznamu filtrovaných adres proveďte následující kroky:

1. Přejděte do nabídky **Settings** (Nastavení) > **Firewall** (Brána firewall) > **URL Filtering** (Filtrování adres URL).
2. Zvolte záznam, který si přejete odstranit, a klikněte na tlačítko **Delete**. Viz obrázek 8-20.

Obrázek 8-20

8.5 Přesměrování portů

Pokud je v CPE aktivní překlad síťových adres (NAT), pouze IP adresa na straně sítě WAN je otevřená a viditelná na internetu. V případě, že má počítač v síti LAN poskytovat služby na internetu (např. být v provozu jako FTP server), je nezbytné aktivovat přesměrování portů, takže veškerý přístup k externímu portu serveru z internetu je přesměrován na server v síti LAN.

8.5.1 Přidání pravidla přesměrování portů

Pro přidání pravidla přesměrování portů proveďte následující kroky:

1. Přejděte do nabídky **Settings (Nastavení) > Firewall (Brána firewall) > Port Forwarding** (Přesměrování portů).
2. Klikněte na tlačítko **Add list** (Přidat seznam).
3. Z rozbalovací nabídky **Service** vyberte požadovanou službu.
4. Z rozbalovací nabídky **Protocol** vyberte protokol.
5. Zadejte rozsah vzdálených portů do pole **Remote port range**.

   Číslo portu může být v rozsahu od 1 do 65535.

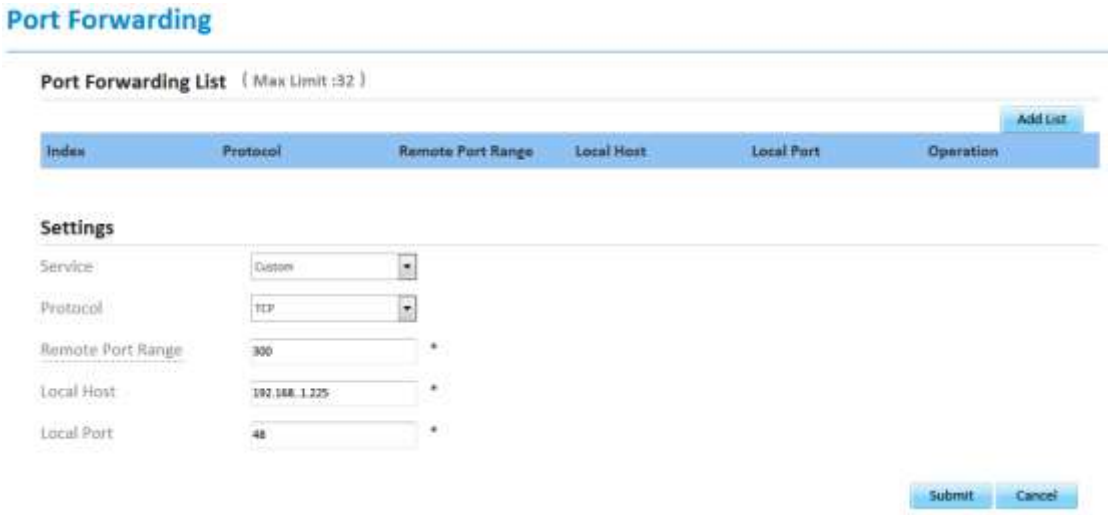
6. Zadejte adresu místního hostitele do pole **Local host.**

   Tato adresa se musí lišit od IP adresy zadané v poli **LAN Host Settings** (Nastavení hostitele LAN), avšak je nutné, aby byly ve stejném síťovém segmentu.

7. Zadejte port místního hostitele do pole **Local port**.

   Číslo portu může být v rozsahu od 1 do 65535.

8. Klikněte na tlačítko **Submit** (Uložit). Viz obrázek 8-21.

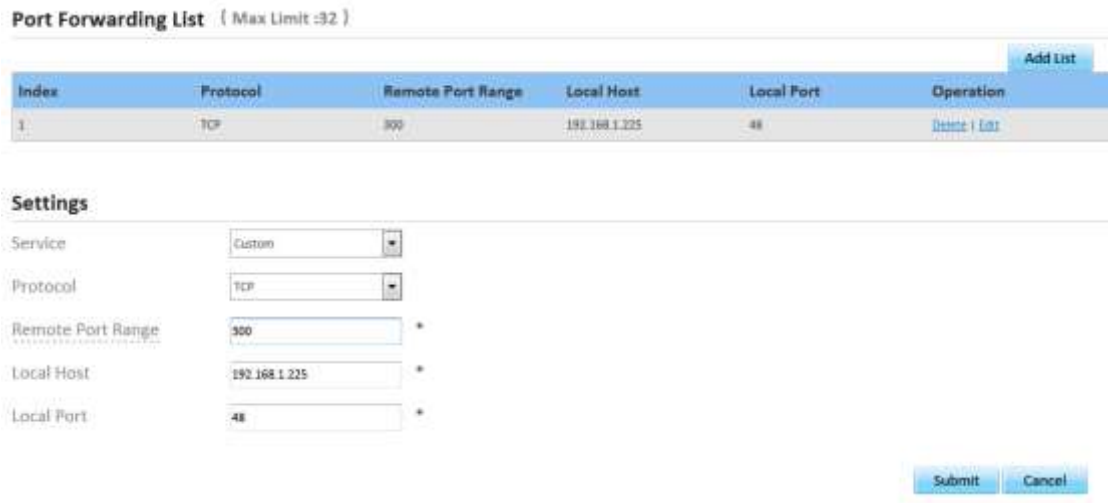


Obrázek 8-21

8.5.2 Upravení pravidla přesměrování portů

Pro upravení pravidla přesměrování portů proveďte následující kroky:

1. Přejděte do nabídky **Settings (Nastavení) > Firewall (Brána firewall) > Port Forwarding (Přesměrování portů).**
2. Zvolte záznam, který si přejete upravit, a klikněte na tlačítko **Edit**.
3. Opakujte kroky 3–7 popsané v předchozím postupu.
4. Klikněte na tlačítko **Submit** (Uložit). Viz obrázek 8-22.



Obrázek 8-82

8.5.3 Odstranění pravidla přesměrování portů

Pro odstranění pravidla přesměrování portů proveďte následující kroky:

1. Přejděte do nabídky **Settings (Nastavení) > Firewall (Brána firewall) > Port Forwarding (Přesměrování portů).**
2. Zvolte záznam, který si přejete odstranit, a klikněte na tlačítko **Delete**. Viz obrázek 8-23.

Obrázek 8-93

8.6 Omezení přístupu

Na této stránce můžete nastavit, kdy může CPE přistupovat k internetu.

8.6.1 Přidání pravidla omezení přístupu

Chcete-li přidat pravidlo omezení přístupu, proveďte následující kroky:

1. Přejděte do nabídky **Settings (Nastavení) > Firewall (Brána firewall) > Access Restriction (Omezení přístupu).**
2. Aktivujte funkci omezení přístupu zaškrtnutím pole Enable.
3. Zadejte název příslušného pravidla.
4. Zadejte adresu MAC příslušného zařízení do pole Device.
5. Vyberte den nebo dny v týdnu, ve kterých chcete omezit přístup k internetu.
6. Zadejte čas, během kterého chcete omezit přístup k internetu. Viz obrázek 8-24

Obrázek 8-24

8.6.2 Upravení pravidla omezení přístupu

Chcete-li upravit pravidlo omezení přístupu, proveďte následující kroky:

1. Přejděte do nabídky **Settings (Nastavení) > Firewall (Brána firewall) > Access Restriction (Omezení přístupu).**

2. Upravte pravidlo. Viz obrázek 8-25

Obrázek 8-25

8.6.3 Odstranění pravidla omezení přístupu

Chcete-li upravit pravidlo omezení přístupu, proveďte následující kroky:

1. Přejděte do nabídky **Settings (Nastavení) > Firewall (Brána firewall) > Access Restriction (Omezení přístupu).**

2. Odstraňte pravidlo. Viz obrázek 8-26

Obrázek 8-26

8.7 Funkce protokolu UPnP

Na této stránce můžete zapnout nebo vypnout funkci protokolu Universal Plug and Play (UPnP).

Chcete-li funkci protokolu UPnP zapnout, proveďte následující kroky:

1. Přejděte do nabídky **Settings** (Nastavení) **> Firewall** (Brána firewall) **> UPnP**.
2. Funkci protokolu **UPnP** zapnete zaškrtnutím pole **Enable**.
3. Klikněte na tlačítko **Submit** (Uložit). Viz obrázek 8-27.

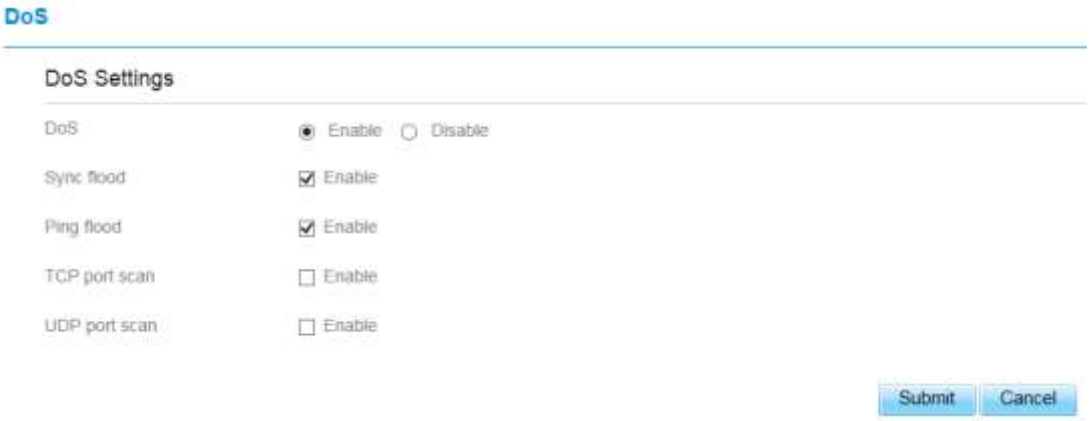
Obrázek 8-27

8.8 Ochrana před odepřením služby (DoS)

Na této stránce můžete zapnout nebo vypnout funkci ochrany před odepřením služby DoS.

Pro zapnutí ochrany před odepřením služby proveďte následující kroky:

1. Přejděte do nabídky **Settings (Nastavení) > Firewall (Brána firewall) > DoS**.
2. Ochranu před odepřením služby **(DoS)** zapnete zvolením možnosti **Enable**.
3. Klikněte na tlačítko **Submit** (Uložit). Viz Obrázek 8-28.


DoS
DoS Settings
DoS
Enable
Disable
Sync flood
Enable
Ping flood
Enable
TCP port scan
Enable
UDP port scan
Enable
Submit
Cancel

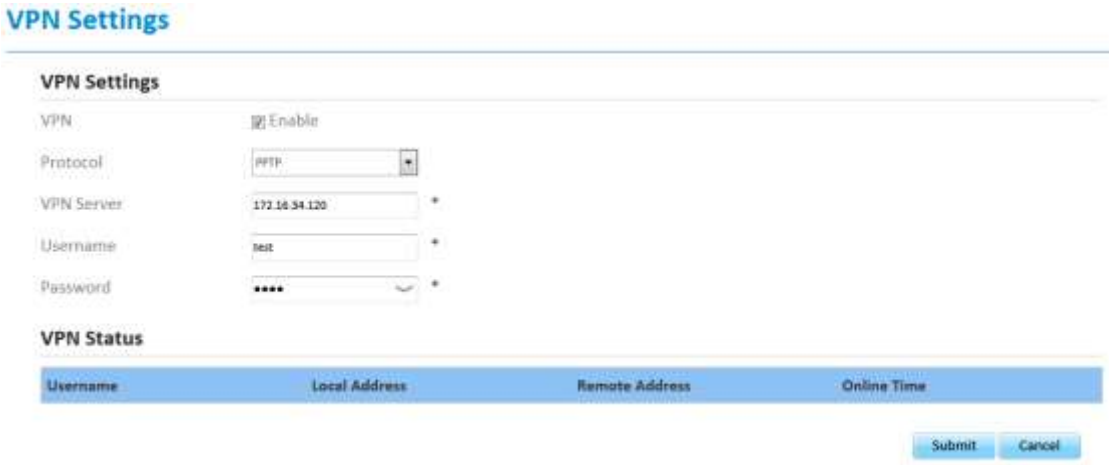
Obrázek 8-28

9 Nastavení VPN

Tato funkce slouží pro nastavení připojení k virtuální privátní síti (VPN).

Pro připojení k VPN proveďte následující kroky:

1. Přejděte do nabídky **VPN Settings** (Nastavení VPN)**.**
2. V oblasti **VPN Settings** (Nastavení VPN) zaškrtněte pole **Enable** u položky **VPN**.
3. Vyberte požadovaný protokol z rozbalovacího seznamu **Protocol**.
4. Zadejte příslušné uživatelské jméno do pole **Username** a heslo do kolonky **Password**.
5. Klikněte na tlačítko **Submit** (Uložit).
6. Stav připojení k síti VPN je zobrazen v tabulce **VPN Status**. Viz obrázek 9-1.



Obrázek 9-1

10 Systém

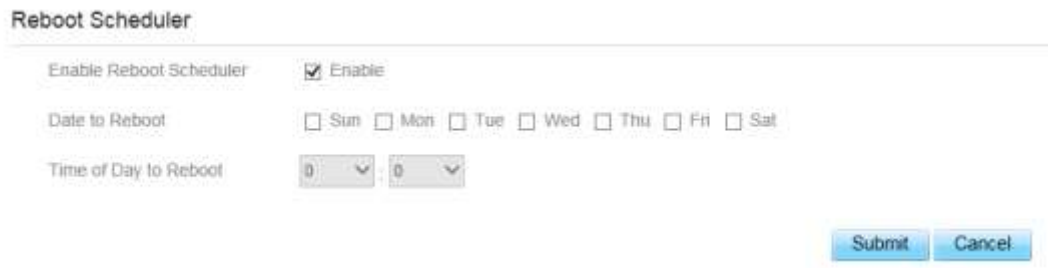
10.1 Údržba

10.1.1 Pravidelné restartování

Tato funkce umožňuje naplánovat automatické restartování CPE. Pro pravidelné restartování CPE proveďte následující kroky:

1. Přejděte do nabídky **Settings** (Nastavení) **> System** (Systém) > **Maintenance** (Údržba).
2. Tuto funkci můžete zapnout zaškrtnutím volby **Enable** a vypnout jejím odškrtnutím.
3. Jakmile bude funkce zapnuta, můžete zvolit den, ve kterém chcete restartování provést, pomocí volby **Date to Reboot**. Analogicky lze nastavit také čas prostřednictvím volby **Time of Day to Reboot**.
4. Klikněte na tlačítko **Submit** (Uložit). Viz obrázek 11-1.

CPE se následně restartuje v nastavený den a čas.

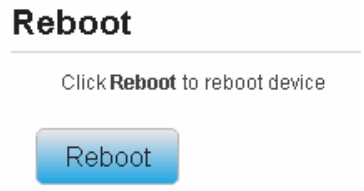


Obrázek 11-1

10.1.2 Jednorázové restartování

Tato funkce umožňuje jednorázově restartovat CPE. Použití provedených změn nastavení proběhne až po restartování CPE. Pro restartování CPE proveďte následující kroky:

1. Přejděte do nabídky **Settings** (Nastavení) **> System** (Systém) > **Maintenance** (Údržba).
2. Klikněte na tlačítko **Reboot** (Restartovat). Viz obrázek 11-2.
   CPE se následně restartuje.



Obrázek 11-2

10.1.3 Obnovení do továrního nastavení

Tato funkce umožňuje obnovit CPE do továrního nastavení.

Pro obnovení do továrního nastavení proveďte následující kroky:

1. Přejděte do nabídky **Settings** (Nastavení) **> System** (Systém) > **Maintenance** (Údržba).
2. Klikněte na tlačítko **Factory Reset.** Viz obrázek 11-3.
   CPE bude obnoven do továrního nastavení.

Obrázek 11-3

10.1.4 Soubor se zálohou konfigurace

Stávající konfiguraci modemu je možné uložit do zálohového souboru. Postup je následující:

1. Přejděte do nabídky **Settings** (Nastavení) **> System** (Systém) > **Maintenance** (Údržba).
2. Klikněte na tlačítko **Download** (Stáhnout) na stránce **Maintenance** (Údržba).
3. Zobrazí se dialogové okno průzkumníka soborů, jehož prostřednictvím zvolte cílovou destinaci a název souboru se zálohou.
4. Klikněte na tlačítko **Save** (Uložit). Viz obrázek 11-4.
   Délka procesu se odvíjí od použitého webového prohlížeče.

Obrázek 11-4

10.1.5 Načtení souboru se zálohou konfigurace

Soubor se zálohou konfigurace je možné načíst a obnovit tak nastavení CPE. Postup je následující:

1. Přejděte do nabídky **Settings** (Nastavení) **> System** (Systém) > **Maintenance** (Údržba).
2. Klikněte na tlačítko **Browse** (Procházet) na stránce **Maintenance** (Údržba).
3. Zobrazí se dialogové okno prohlížeče souborů, jehož pomocí najděte soubor se zálohou.
4. Klikněte na tlačítko **Open** (Otevřít).
5. Dialogové okno se zavře. V boxu vedle tlačítka pro načtení souboru se zálohou se zobrazí název souboru se zálohou konfigurace a cesta k němu.
6. Klikněte na tlačítko **Upload** (Nahrát). Viz obrázek 11-5.

Dojde k nahrání souboru se zálohou konfigurace. CPE se následně automaticky restartuje.

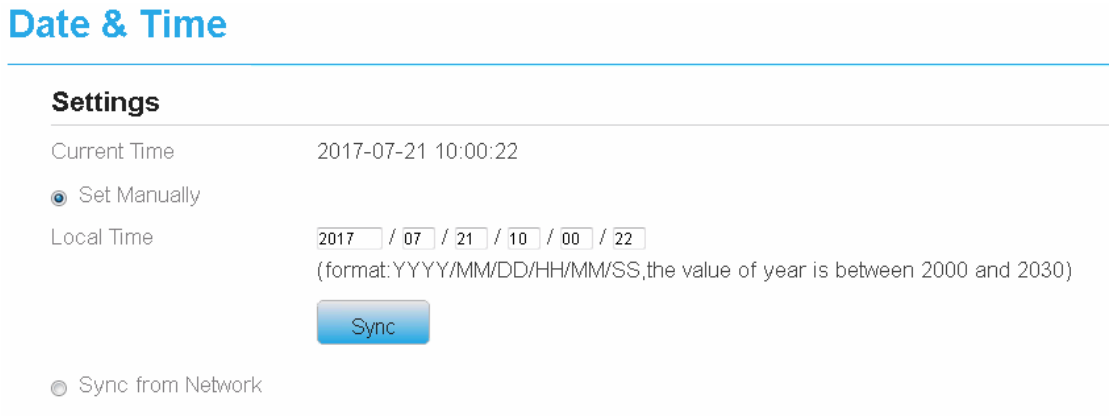
Obrázek 11-5

10.2 Datum a čas

Systémový čas modemu můžete nastavit ručně, nebo jej získat automaticky ze sítě. Pokud zvolíte možnost **Sync from Network**, bude modem pravidelně získávat čas ze serveru časového protokolu NTP (Network Time Protocol). Pokud zaškrtnete možnost Enable daylight savings time (DST), bude modem současně respektovat střídání letního a zimního času.

Pro nastavení data a času proveďte následující kroky:

1. Přejděte do nabídky System (Systém) > Date & Time (Datum a čas).
2. Vyberte možnost **Set manually** (Nastavit ručně).
3. Zadejte čas do polí **Local time** (Místní čas), případně klikněte na tlačítko **Sync** pro vyplnění aktuálního času z počítače, který aktuálně používáte.
4. Klikněte na tlačítko **Submit** (Uložit). Viz obrázek 11-7.

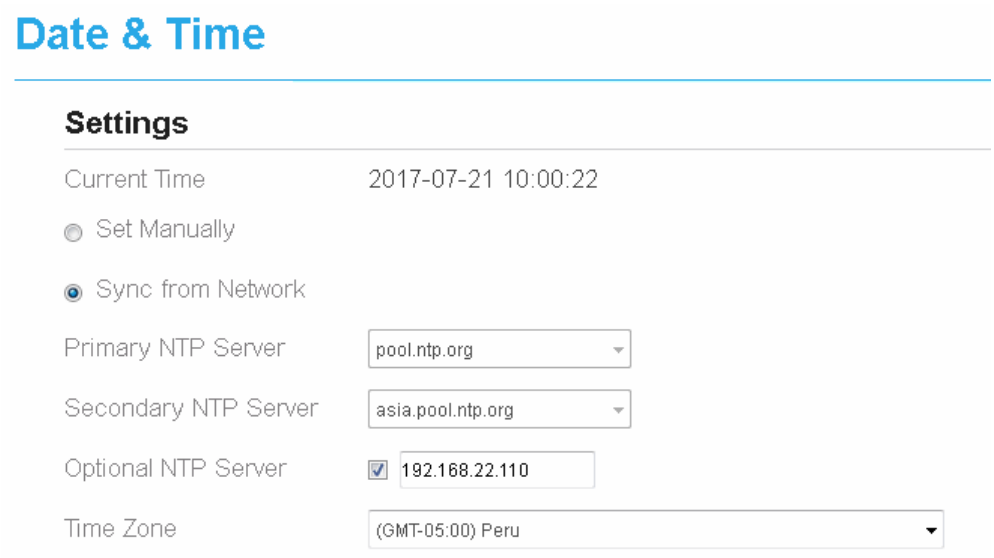


Obrázek 11-7

Pro automatickou synchronizaci času proveďte následující kroky:

1. Přejděte do nabídky **System** (Systém) > **Date & Time** (Datum a čas).
2. Vyberte možnost **Sync from Network** (Synchronizovat ze sítě).
3. Z rozbalovací nabídky **Primary NTP Server** vyberte primární NTP server pro synchronizaci času.
4. Z rozbalovací **Secondary NTP Server** vyberte druhý NTP server pro synchronizaci času.

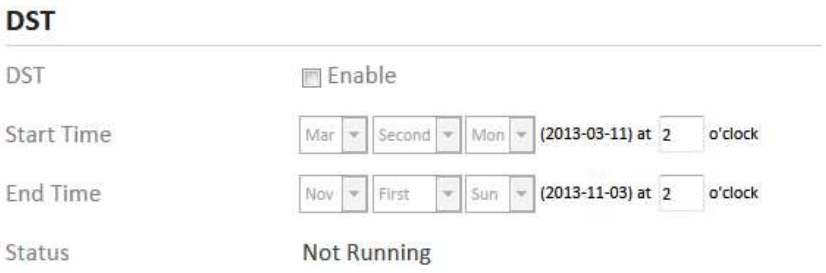
5. Pokud nechcete používat žádný z nabízených NTP serverů, zaškrtněte položku **Optional NTP Server** a zadejte IP adresu požadovaného časového serveru.
6. Vyberte z rozbalovací nabídky **Time zone** časovou zónu, ve které se nacházíte.
7. Klikněte na tlačítko **Submit** (Uložit). Viz obrázek 11-8.



Obrázek 11-8

Pro nastavení střídání letního a zimního času proveďte následující kroky:

1. Přejděte do nabídky **Settings** (Nastavení) **> System** (Systém) > **Date & Time** (Datum a čas).
2. Zaškrtněte volbu **Enable** pro aktivaci střídání letního a zimního času.
3. Zadejte čas začátku a čas konce do pole **Start Time**, resp. **End Time**.
4. Klikněte na tlačítko **Submit** (Uložit). Viz obrázek 11-9.



Obrázek 11-9

Modem bude respektovat střídání letního a zimního času v závislosti na časové zóně.

10.3 Služba DDNS

Služba DDNS (Dynamic Domain Name Server) se používá k mapování dynamické IP adresy uživatele k fixnímu poskytovateli služby DNS.

Pro změnu nastavení služby DDNS proveďte následující kroky:

1. Přejděte do nabídky **System** (Systém) **> DDNS**.
2. Službu DDNS zapnete zaškrtnutím pole **Enable**.
3. Zvolte poskytovatele služby, DynDNS.org nebo oray.com, v rozbalovací nabídce **Service provider**.
4. Vyplňte pole **Domain name** (Doménové jméno) a **Host name** (Název hostitele). Například, pokud je adresa od vašeho poskytovatele služeb test.customtest.dyndns.org, zadejte jako doménové jméno „customtest.dyndns.org“ a jako název hostitele „test“.
5. Zadejte uživatelské jméno a heslo do polí **User name**, resp. **Password.**
6. Nastavte interval obnovení do pole **Refresh time**.
7. Zaškrtněte v případě potřeby možnost **Enable Wildcard** (Povolení divoké karty).
8. Zaškrtněte v případě potřeby možnost **WAN IP and domain verification** (Ověření IP adresy a domény WAN).
9. Klikněte na tlačítko **Submit** (Uložit). Viz obrázek 11-10.

Obrázek 11-10

10.4 Diagnostika

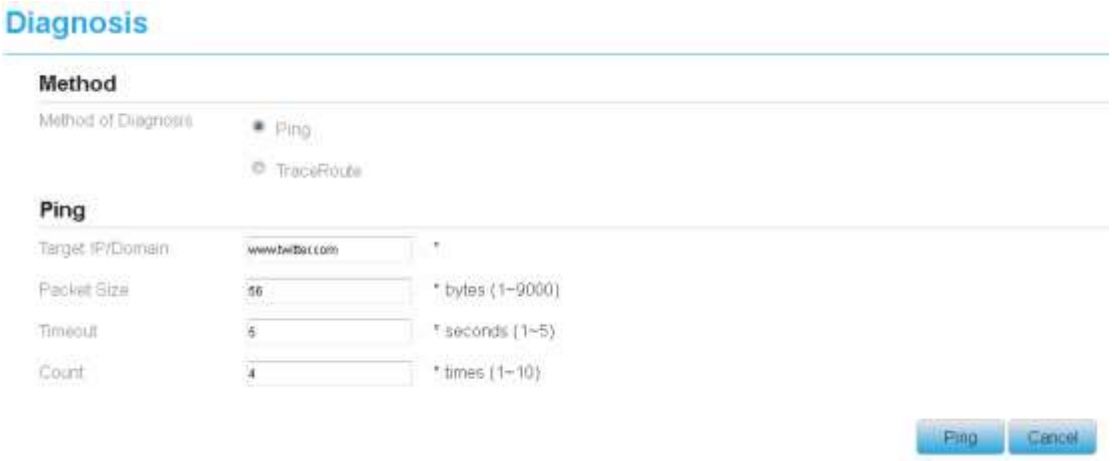
Pokud modem nepracuje správně, je možné pomocí diagnostických nástrojů na stránce **Diagnosis** provést ověření příčiny problému.

10.4.1 Ping

Pokud připojení k internetu nebude úspěšné, pokuste se identifikovat zdroj problému pomocí příkazu ping. Postup je následující:

1. Přejděte do nabídky **Settings** (Nastavení) **> System** (Systém) > **Diagnosis** (Diagnostika).
2. V sekci **Method** (Metoda) zvolte možnost **Ping**.
3. Zadejte cílové doménové jméno do pole **Target IP/Domain**, např. www.google.com.
4. Nastavte velikost paketu do pole **Packet size** a časový interval vypršení do pole **Timeout**.
5. Nastavte počet opakování příkazu do pole **Count**.
6. Klikněte na tlačítko **Ping**. Viz obrázek 11-12.

Vyčkejte, dokud nebude provedení příkazu ping dokončeno. Výsledek se zobrazí v textovém poli v rámečku Results.



Obrázek 11-12

10.4.2 Příkaz traceroute

Pokud připojení k internetu nebude úspěšné, pokuste se identifikovat zdroj problému pomocí příkazu traceroute. Postup je následující:

1. Přejděte do nabídky **Settings** (Nastavení) **> System** (Systém) > **Diagnosis** (Diagnostika).
2. V sekci **Method** (Metoda) zvolte možnost **Traceroute**.
3. Zadejte cílové doménové jméno do pole **Target IP/Domain**. Příklad: www.google.com.
4. Nastavte maximální počet skoků (hops) do pole **Maximum hops** a časový interval vypršení do pole **Timeout**.
5. Klikněte na tlačítko **Traceroute**. Viz obrázek 11-13.

Vyčkejte, dokud nebude provedení příkazu traceroute dokončeno. Výsledek se zobrazí v textovém poli v rámečku Results.

Obrázek 11-13

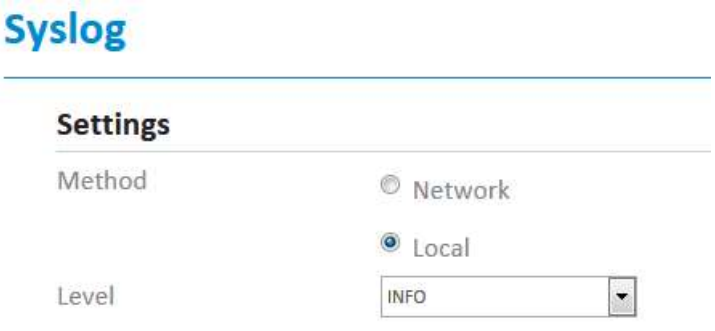
10.5 Systémový log

Systémový log slouží k záznamu operací uživatele a klíčových událostí, které nastaly při běhu modemu.

10.5.1 Lokální

Pro nastavení systémového logu na lokální proveďte následující kroky:

1. Přejděte do nabídky **System** (Systém) > **Syslog** (Systémový log).
2. V oblasti **Settings** (Nastavení) zvolte metodu **Local** (Lokální).
3. Pomocí rozbalovací nabídky **Level** zvolte úroveň logování.
4. Klikněte na tlačítko **Submit** (Uložit). Viz obrázek 11-15.



Obrázek 11-15

Zobrazení lokálního systémového logu

Lokální systémový log zobrazíte následujícími kroky:

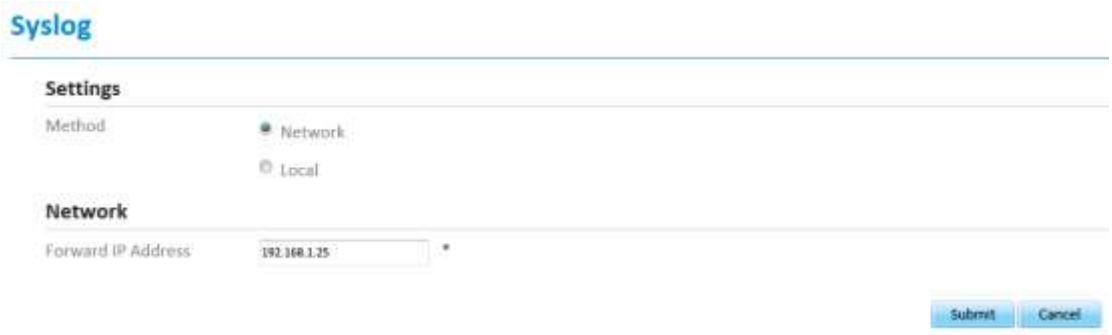
1. Zadejte požadované klíčové slovo do pole **Keyword**.
2. Klikněte na tlačítko **Pull** (Získat). Zobrazí se odpovídající výsledky ze systémového logu.

10.5.2 Síťový

Pro nastavení systémového logu na síťový proveďte následující kroky:

1. Přejděte do nabídky **System** (Systém) > **Syslog** (Systémový log).
2. V oblasti **Settings** (Nastavení) zvolte metodu **Network** (Síťový).
3. Pomocí rozbalovací nabídky **Level** zvolte úroveň logování.
4. Do pole **Forward IP address** zadejte IP adresu, na kterou si přejete log odesílat.
5. Klikněte na tlačítko **Submit** (Uložit). Viz obrázek 11-16.

Systémový log bude odesílán na zadané klientské zařízení prostřednictvím sítě.



Obrázek 11-16

10.6 Nastavení webových parametrů

Pro nastavení webových parametrů proveďte následující kroky:

1. Přejděte do nabídky **Settings** (Nastavení) **> System** (Systém) **> Web settings** (Webová nastavení)
2. Zaškrtněte položku **HTTP Enable**. Pokud tato položka zaškrtnuta nebude, nebudete se moci přihlásit k webovému rozhraní pro správu pomocí protokolu HTTP ze strany WAN.
3. Zadejte číslo portu do pole **HTTP Port**. Pokud si přejete změnit číslo portu pro přihlášení, můžete zadat číslo nového portu do tohoto pole. Výchozím portem HTTP je 80.
4. Zaškrtněte položku **HTTPS Enable**. Pokud se chcete k webovému rozhraní pro správu přihlašovat pomocí protokolu HTTPS ze strany WAN, je zapotřebí tuto funkci povolit.
5. V případě, že se chcete přihlašovat k webovému rozhraní pro správu ze sítě WAN, je nutné zaškrtnout také volbu **Enable** u položky **Allowing login from WAN**.
6. Zadejte číslo portu do pole **HTTPS Port**.
7. Zadejte do pole **Refresh Time** požadovaný interval obnovení.
8. Zadejte do pole **Session Timeout** požadovaný časový interval vypršení relace.

9. Z rozbalovací nabídky **Language** vyberte požadovaný jazyk.
10. Klikněte na tlačítko **Submit** (Uložit) Viz obrázek 11-17.

Obrázek 11-17

10.7Účet

Pomocí této nabídky můžete změnit přihlašovací údaje uživatele. Po změně hesla bude zapotřebí nové heslo zadat již při příštím přihlášení.

Pro změnu hesla proveďte následující kroky:

1. Přejděte do nabídky **Settings** (Nastavení) **> System** (Systém) > **Account** (Účet).
2. Z rozbalovací nabídky **Username** vyberte uživatelské jméno, u nějž si přejete změnit heslo. Pokud chcete změnit heslo běžného uživatele, je zapotřebí zaškrtnout možnost **Enable User**.
3. Dále zadejte stávající heslo do pole **Current Password**, nové heslo do pole **New Password** a opakujte zadání nového hesla pro potvrzení do pole **Confirm Password**.
4. Pole **New Password** a **Confirm Password** musí obsahovat minimálně 5 a maximálně 15 znaků.
5. Klikněte na tlačítko **Submit** (Uložit) Viz obrázek 11-18.

Obrázek 11-18

10.8Odhlášení

Pro odhlášení z webového rozhraní pro správu proveďte následující kroky:

1. Přejděte do nabídky **System** (Systém) a klikněte na **Logout** (Odhlásit se).
2. Budete vráceni na stránku s přihlášením.

11 Často kladené dotazy

Indikátor POWER nesvítí.

- Ujistěte se, že je napájecí kabel správně připojen, a že je zařízení správně zapnuto.
- Ujistěte se, že použitý napájecí adaptér je kompatibilní s CPE.

Přihlášení do webového rozhraní pro správu není možné provést.

- Ujistěte se, že je CPE spuštěno.
- Ověřte, že je CPE správně připojeno k počítači prostřednictvím síťového kabelu. Pokud problém přetrvá, obraťte se na autorizované servisní středisko.

Modemu se nedaří navázat připojení k bezdrátové síti.

- Zkontrolujte, zda je napájecí adaptér správně připojen.
- Ověřte, že se CPE nachází na otevřeném místě bez překážek, jako jsou betonové nebo dřevěné stěny.
- Ujistěte se, že se CPE nachází v dostatečné vzdálenosti od domácích spotřebičů, které generují silné elektromagnetické pole, jako jsou mikrovlnné trouby, ledničky nebo satelity.

Pokud problém přetrvá, obraťte se na autorizované servisní středisko.

Napájecí adaptér CPE se přehřívá.

- Modem se bude v případě dlouhé doby provozu zahřívat. Z toho důvodu doporučujeme CPE vypínat ze síťové zásuvky, jakmile jej nebudete používat.
- Zajistěte důkladné odvětrávání CPE a udržujte jej mimo přímé sluneční světlo.

Nastavení modemu bylo resetováno na výchozí hodnoty.

- Pokud dojde během konfigurace k neočekávanému vypnutí napájení CPE, může se stát, že veškerá nastavení budou obnovena na výchozí hodnoty.
- Rychlé obnovení požadovaných nastavení můžete provést nahráním konfiguračního souboru ze zálohy.